

دورة التخفي والتصفح الآمن للإنترنت.

مقدمة عن الدورة.

محتويات الدرس :

1- أسباب عمل هذه الدورة.
2- فهرس الدورة.



مقدمة :

معلومات مهمة يجب معرفتها.

بعد أن أصبحت شبكة الإنترنت جزء لا يتجزأ من حياتنا كـ عوام, وكـ مناصرين للدولة الإسلامية والمجاهدين بشكل خاص

فهناك الكثير من الأمور التي يجب أن نَعيها عند استخدام الإنترنت والمخاطر التي ممكن أن نقَع بها.

فسمعنا كثيراً من الاخبار التي تقول أنو حكومة البلد الفلاني اعتقلت أشخاص لقيامهم بأعمال غير قانونية على الإنترنت.

وسمعنا أيضاً أخبار باعتقال اخوة في بلد عربي بسبب مناصرتهم للدولة الإسلامية على الإنترنت ونشرهم أخبارها.

لذلك رأينا وجوب القيام بعمل يوضح مخاطر الإنترنت وكيفية حماية الخصوصية وتعقيد المهمة على الحكومات بالتجسس.



مقدمة :

معلومات مهمة يجب معرفتها.

ولذلك سنتطرق بهذه الدورة الى ذكر خطوات بسيطة ومتقدمة في الحماية والتخفي.

وننصح جميع المناصرين بالقيام بهذه الخطوات, لتأمين خصوصيتهم على شبكة الإنترنت.

اولاً - هناك عدة أمور يجب أن نعيها, وهناك كثير من الناس لديها مفاهيم خاطئة عنها.

- يجب أن نعي تماماً أن طرق حماية هويتنا على الإنترنت كثيرة ويجب مراعاة أغلبها لنضمن مجهولية أكبر على شبكة الإنترنت.

فلا تعتقدوا أنكم اذا أخفيتم (الآي بي) الخاص بكم فأنكم بأمان تام, فهذا الكلام خاطئ.

مقدمة :

معلومات مهمة يجب معرفتها.

فإخفاء «الآي بي» مجرد تمويه بسيط وذلك لا يأمن أي حماية لخصوصيتنا والمعلومات التي نرسلها ونستقبلها.

- أيضاً البعض يظن أن باستعماله «الشبكات الخاصة الافتراضية VPN» فإنه بمأمن عن الخطورة.

وذلك فيه بعض الخطأ, فصحيح أن «الشبكات الخاصة الافتراضيةVPN» تأمن نوع من التشفير على بياناتك .

لكن هذا لا يكفي, وسأتعمق بذلك لاحقاً ان شاء الله.

وان شاء الله سنوضح في هذه الدورة عدة نقاط تأمن لنا خصوصية على الإنترنت قدر الإمكان.

مقدمة :

معلومات مهمة يجب معرفتها.

فنية الإسلام

فبدايةً سنقوم بشرح عدة أمور لتأمين خصوصيتكم على الحاسوب الشخصي وستكون البرامج التي سنستخدمها مجانية.

و تفييدكم هذه الخطوات بحال أردتم استخدام الحسابات الشخصية وتصفح الإنترنت بشكل أمن.

وبعدها سنطرح طرق متقدمة لتأمين خصوصية أعلى من خلال عدة أمور إضافية لما سبق.

وبحال كنت تريد خصوصية عالية جداً وتريد أمان شبه تام للقيام بأعمال سرية للغاية

فأنت بحاجة لأمور متقدمة أكثر والكثير من هذه الأمور لن تكون مجانية.

فئة الإسلام

مقدمة :

معلومات مهمة يجب معرفتها.

فقد يحتاج الأمر الى اشتراكات في بعض الخدمات التي سنتحدث عنها لاحقاً ومنها سيكون مجاني لفترة تجريبية.

وبعد قيامنا بهذه الخطوات فإننا نُعقد المهمة بشكل كبير ونجعلها صعبة على من يريد أن يتجسس علينا.

لأنه تأكدوا تماماً, انه لا يوجد شيء اسمه حماية تامة.

وكل ما سنقوم به هو لتعقيد المهمة على الأمنين, فأن اتباعك للخطوات بشكل سليم

وإخفاء أثرك على الإنترنت سيجعل مهمة الأمنين معقدة جداً.

مقدمة :

معلومات مهمة يجب معرفتها.

فنية الإسلام

مقدمة :

معلومات مهمة يجب معرفتها.

ب- الخطوات المتقدمة:

1- ما هي التوزيعة «تايلس».

2- ما هو الـ «آر دي بي» وكيف أحصل عليه.

3- التشفير اليدوي للرسائل والملفات.



دورة التخفي والتصفح الآمن للإنترنت.

الدرس الأول.

محتويات الدرس:

1- تعريف برنامج «تور» وطريقة عمله.

2- تعريف شبكات «VPN» وطريقة عملها.

3- ما الفرق بينهما.



ما هو برنامج «تور» وما هي شبكات الـ «VPN»:

ما هو بروتوكول الـ «HTTPS».

فعندما تذهب الى متصفحك وتكتب الموقع الذي تريد الدخول إليه ونفرض أنك كتبت google.com

فتلقائيا سيتحول الى https://www.google.com وهذا يعني ان هذا الموقع يعمل مع بروتوكول https.

واغلب المواقع التي نتصفحها تعمل على http وبحال لم يظهر بروتوكول بشريط العنوان فمعناه ان الموقع يستخدم http

لا أريد أن اتعمق أكثر بخصوص البروتوكولات فمن أراد التعمق عليه بالبحث بالإنترنت عن ذلك.

ولذلك ننصح دائما بعدم إرسال معلومات هامة كـ كلمات مرور او غيرها على مواقع لا تعمل ببروتوكول https.

ما هو برنامج «تور» وما هي شبكات الـ «VPN»:

ما هي الشبكات الخاصة الافتراضية الـ «VPN»

VPN: اختصار لـ «الشبكة الخاصة الافتراضية» و يكتسي أهمية كبيرة لدى مستخدمي الإنترنت لما له من مزايا،

كالقدرة على ولوج المواقع المحظورة في منطقتك أو تصفح الإنترنت بأمان.

فعندما تربط حاسوبك بخدمة **VPN** أكانت مجانية أو مدفوعة، فإن كل البيانات ترسل مشفرة الى سيرفر الخدمة الخاص،

وهذا يجعل حاسوبك يتصرف وكأنه ومتواجد بنفس خادم الـ **VPN** ، مما يتيح إمكانية تصفح الويب بأمان وسرية.

أي اذا كان الخادم ببريطانيا سيظهر حاسوبك وكأنه هناك، وتكمن أهمية هذه الخاصية في القدرة على ولوج المواقع المحظورة.



ما هو برنامج «تور» وما هي شبكات الـ «VPN»:

ما هي الشبكات الخاصة الافتراضية الـ «VPN»

ولمن التعمق أكثر بخصوص الـ VPN فمن أراد التعمق فعليه بالبحث بالإنترنت

وبخصوص IP Address ؛ فهو يعتبر المعرف الرقمي لأي جهاز مرتبط بشبكة معلوماتية تعمل بحزمة بروتوكولات الإنترنت،

يقابل عنوان الآي بي مثلا في شبكات الهاتف رقم الهاتف، فكل جهاز يتصل بشبكة يكون له ip خاص به

داخل هذه الشبكة من أي نوع كانت، ولكل شيء على الشبكة ip خاص به سواء كان موقع أو سيرفر أو أي شيء متصل.

أما بالنسبة للأخوة الذين يسألون عن "البروكسي" واستخدامه، فلا ننصح باستخدامه أبدا فهو غير محمي ولا يشفر بياناتك.

فنية الإسلام

ما هو برنامج «تور» وما هي شبكات الـ «VPN»:

ما هي شبكات تخفيه رقم شبكة الـ «VPN»

يستخدم البروكسي فقط في الحالات البسيطة كـ الدخول لموقع ما محظور في بلدك وتريد تجاوز الحظر و الدخول الى الموقع.

وفي أقل تقدير ان لم تستطع تشغيل «تور» وواجهت مشاكل معه, فلتستعمل VPN وهناك شركات تقدم خدمات مجانية.

و أبرز الشركات التي تقدم خدمة مجانية هي Hotspot Shield

ولكن أبرز مساوئ هذه الشركات هي ظهور إعلانات أثناء التصفح + تقوم بتخزين سجلات لما قمت بعمله.

ومن الصعب وجود شركات تقدم خدمة مجانية بدون تخزين سجلات فأغلبها يكون بشكل مدفوع.



ما هو برنامج «تور» وما هي شبكات الـ «VPN»:

الفرق بين «تور» و الـ «VPN»

- لا يمكن تتبع عنوانكم الحقيقي.
- شبكة كبيرة وموزعة حول العالم، ما يجعل من شبه المستحيل أن يتم مهاجمتها وإيقافها.
- يمكنكم من التحايل على الموقع الجغرافي، ولكن من الممكن للمواقع معرفة أنكم تستخدمون تور.
- مجاني.

- سريع.
- التحايل على الموقع الجغرافي (تغيير الموقع بالنسبة للمواقع التي تزورونها) سهل جدا.
- من الممكن استخدامه للتحميل من مواقع مشاركة الملفات مثل الـ «تورنت» في حال كان مزود الخدمة لا يسمح بذلك.

ما هو برنامج «تور» وما هي شبكات الـ «VPN»:

الفروق بين «تور» و «VPN»

- بطيء، بسبب اتصاله بعدد من العقد، وهذه العقد تختلف سرعتها وقد تتواجد في أماكن متباعدة من العالم.
- غير مناسب للتحميل، على الرغم من أنه غير ممنوع، ولكن بسبب بطء الشبكة سيكون اتصالكم بطيئا.

- يستطيع مزود خدمة الشركة معرفة عنوانكم الحقيقي والبيانات التي ترسلونها.
- بعض المزودات تقوم بتخزين سجلات بياناتكم وتحتفظ بها لمدة معينة.
- تبادل البيانات في الاشتراك المجاني محدود غالبا، وقد تختلف السرعة مقارنة بالحسابات المدفوعة.

ما هو برنامج «تور» وما هي شبكات الـ «VPN»:

الفرق بين «تور» و «VPN»

ومع ذلك لا ننصح باستخدام شبكات VPN لأن معظم الشركات التي تعطي الخدمة بشكل مجاني تخزن سجلات عنك.

أما إذا أردت استخدام هذه الشبكات فعليك بالبحث عن شركات لا تخزن سجلات وهذه الشركات تكون خدمتها مدفوعة ولن تعطيك خدمة بشكل مجاني، وهذا سيشكل عائقاً لدى الكثيرين.

وبحالة كنت لا تقوم بشيء سري، و أردت فقط دخول موقع محظور أو شيء بسيط فلا بأس باستخدامه.

ما هو برنامج «تور» وما هي شبكات الـ «VPN»:

شرح برنامج «تور» وطريقة عمله

تم عمل برنامج «تور» ليؤمن مجهولية الاتصال والخصوصية والأمان لنشاط المستخدمين على الإنترنت

حيث يقوم البرنامج بربط المستخدم بشبكة «تور» التي تتألف من مجموعة «عُقد» متداخلة وأنفاق افتراضية عبر الإنترنت

يتم الاتصال عبر هذه «العُقد» للحصول على خصوصية عالية وتأمين المستخدمين من تسجيل تحركاتهم على شبكة الأنترنت والمواقع التي يزورونها.
كما تحميهم من محاولات التعقب وتحديد الهوية وعمليات التجسس التي يمكن أن يقوم بها أفراد أو شركات أو حكومات

يتوفر «تور» بعدة إصدارات تعمل في بيئات مختلفة كـ ويندوز ولينوكس ونسخة هواتف للاندرويد.

ما هو برنامج «تور» وما هي شبكات الـ «VPN»:

ما هي شبكة «تور» وما هي العقد «NODES»

شبكة «تور» هي مجموعة كبيرة من الأجهزة التي يشغلها متطوعون حول العالم، تسمى هذه الأجهزة بـ «عقد».

يتم اختيار هذه العقد من «تور» بشكل عشوائي، وفي كل عملية اتصال يوجد 3 عقد: عقدة دخول، عقدة وسطى، وعقدة خروج.

فالطريقة التي يعمل بها «تور» تمنع أي شخص يراقب اتصالكم من معرفة المواقع والخدمات التي تزورونها.

كما تمنع أيضا هذه المواقع من معرفة موقعكم الجغرافي الحقيقي.

صورة توضح طريقة الاتصال بشبكة «تور»



ما هو برنامج «تور» وما هي شبكات الـ «VPN»:

ما هي شبكة «تور» وما هي العقد «NODES»

How Tor Works

عقد تور
Tor node
خط غير مشفر
unencrypted link
خط مشفر
encrypted link

Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear

Jane

Bob

حاسوبك



ما هو برنامج «تور» وما هي شبكات الـ «VPN»:

ما هي شبكة «تور» وما هي نقاط «NODES»

عقدة الدخول: في «تور» تعرف موقعكم الجغرافي، فيما لا تعرف البيانات التي يتم إرسالها لأنها تكون مشفرة قبل دخولها.

العقدة الوسطى: لا تعرف أي معلومات (لا مكانكم الجغرافي، ولا البيانات التي أرسلتموها، ولا الموقع الذي تتوجهون إليه)

العقدة الوسطى تعرف فقط أن عليها استقبال البيانات من عقدة الدخول، وتمريرها إلى عقدة الخروج.

عقدة الخروج: تقوم بفك تشفير البيانات وتمريرها إلى الموقع، فعقدة الخروج تعرف الموقع الذي تودون زيارته، والبيانات التي ترسلونها لتمريرها إلى الموقع.

لكن في حال التعامل مع موقع يدعم « HTTPS» فإن عقدة الخروج لن تعرف سوى الموقع الذي تريدون زيارته فقط.



ما هو برنامج «تور» وما هي شبكات الـ «VPN»:

ما هو بروتوكول الـ «HTTPS»

وهو بروتوكول شبيه الى حد ما بالبروتوكول HTTP لكنه يستعمل SSL

وهذه البروتوكولات تستعمل لإرسال البيانات بين جهازك وسيرفرات الإنترنت وهذه المعلومات تظهر لك عن طريق المتصفح

أما الفرق بين http وبين https هو بسيط جدا, فالأول يرسل البيانات كما هي دون تشفير

فلنفترض ان هناك طرفان الطرف الأول A والطرف الثاني B , فالطرف الأول يريد مراسلة الطرف الثاني

مثلا كإرسال كلمة مرور او اي شيء, فعندما يأتي من يحاول التجسس ان يرى ما يتم إرساله فسوف تظهر له البيانات كما هي



ما هو برنامج «تور» وما هي شبكات الـ «VPN»:

ما هو بروتوكول الـ «HTTPS»

بحال استعمل بروتوكول http ستكون النتيجة كالتالي:

مرسل كلمه السر

مستقبل كلمة السر

Bahrain

HTTP

يخترق الهكر الوصلة بين الطرفين وسيعرف كلمة السر التي تم ادخلها

Bahrain



ما هو برنامج «تور» وما هي شبكات الـ «VPN»:

ما هو بروتوكول الـ «HTTPS»

اما اذا كان يستخدم بروتوكول https فهو يقوم بتشفير البيانات عن طريق شهادة SSL تتكون من مفتاح عام ومفتاح خاص.

ويستخدم المفتاح العام لتشفير المعلومات ويستخدم المفتاح الخاص لفك تشفيرها.

عندما يتصل المتصفح الخاص بك بموقع آمن ، يقوم الخادم بإرسال المفتاح العام للمتصفح لتنفيذ عملية التشفير.

المفتاح العام متاح للكل ولكن المفتاح الخاص (الذي يستخدم لفك التشفير) هو سري.

ولنفرض انت تريد المراسلة لكن ببروتوكول https سيكون الوضع كالتالي:



ما هو برنامج «تور» وما هي شبكات الـ «VPN»:

ما هو بروتوكول الـ «HTTPS»

بحال استعمل بروتوكول https ستكون النتيجة كالتالي:

مستقبل كلمة السر

مرسل كلمة السر

HTTPS

Bahrain

Yt75@2Rkwd

Bahrain

Hacker

يخترق الهكر الوصلة بين الطرفين و سيحصل على كلمة مرور بهذا الشكل : Yt75@2Rkwd

فهي مشفرة ولا يمكن معرفتها!



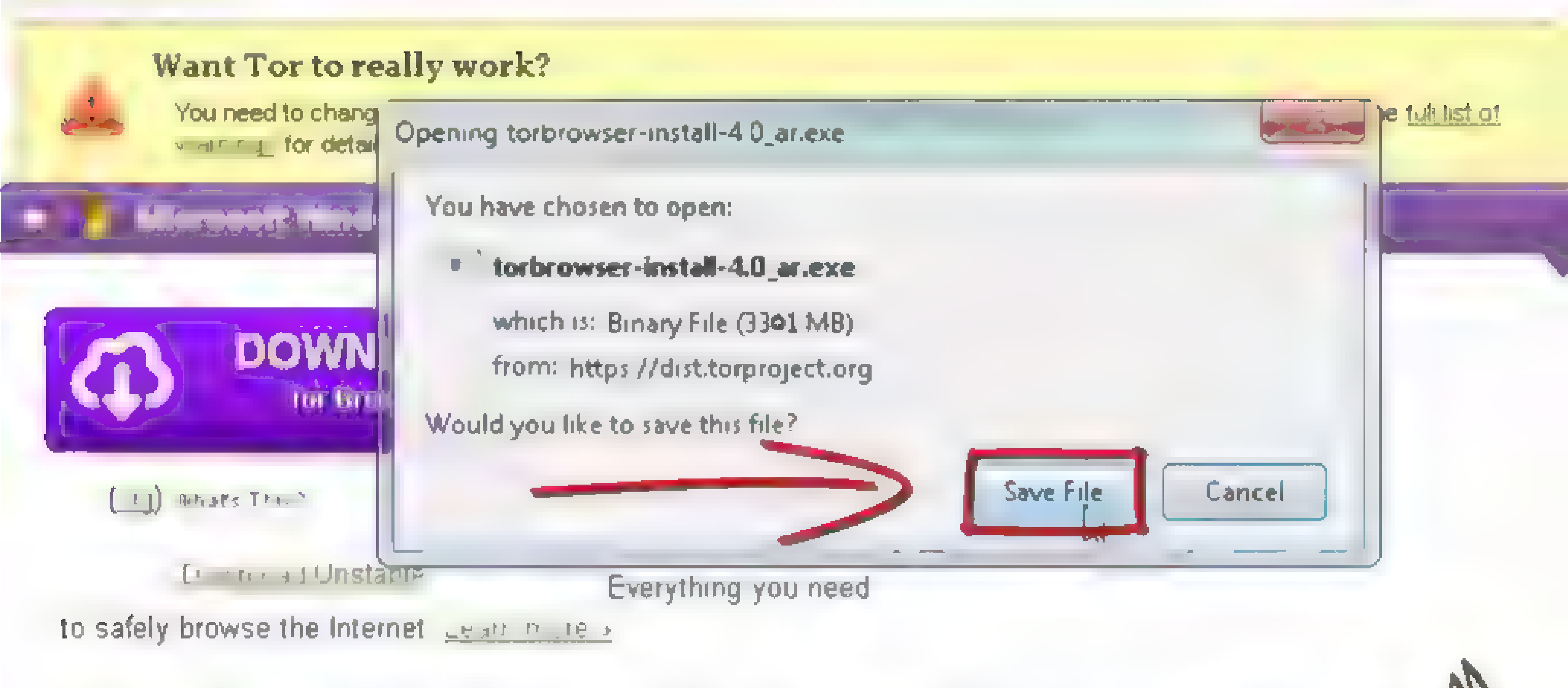
دورة التخفي والتصفح الآمن للإنترنت.

الدرس الثاني:

1- تعريف بحزم برنامج «تور».

2- تحميل وتنصيب الحزمة التي سنتعامل معها

3- الاتصال بشبكة «تور» وتخطي الحظر بحال وجوده.



ثم تظهر لنا نافذة جديدة لحفظ البرنامج المراد تنزيله ونضغط على حفظ

فتية الإسلام


Google
torbrowser-install-4.0_ar.exe
Donate to Tor
$ 5
ويبدأ المتصفح بتحميل البرنامج



حِزم برنامج «تور» وكيفية التعامل مع البرنامج :

وبحال كان الموقع محظور وأردت التحميل من الرابط البديل الذي ذكرناه سابقاً, كل ما عليك هو الدخول للرابط

ثم الضغط على Direct Download Link كما في الصورة التالية:

Tor Browser Bundle

Download Now

Quick Specs

4.0

620 923

32.89MB

7.15

حِزم برنامج «تور» وكيفية التعامل مع البرنامج :





حِزم برنامج «تور» وكيفية التعامل مع البرنامج :

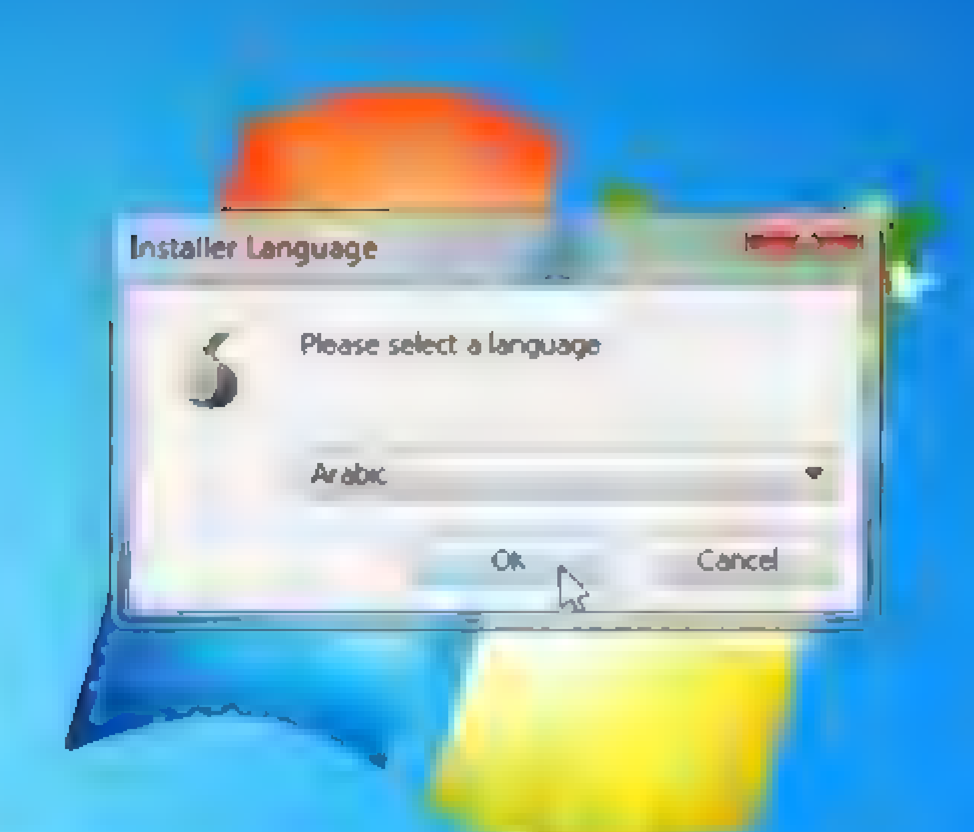
كيفية التعامل مع البرنامج، [illegible]

دعونا نشاهد شرح بسيط لتنصيب البرنامج.



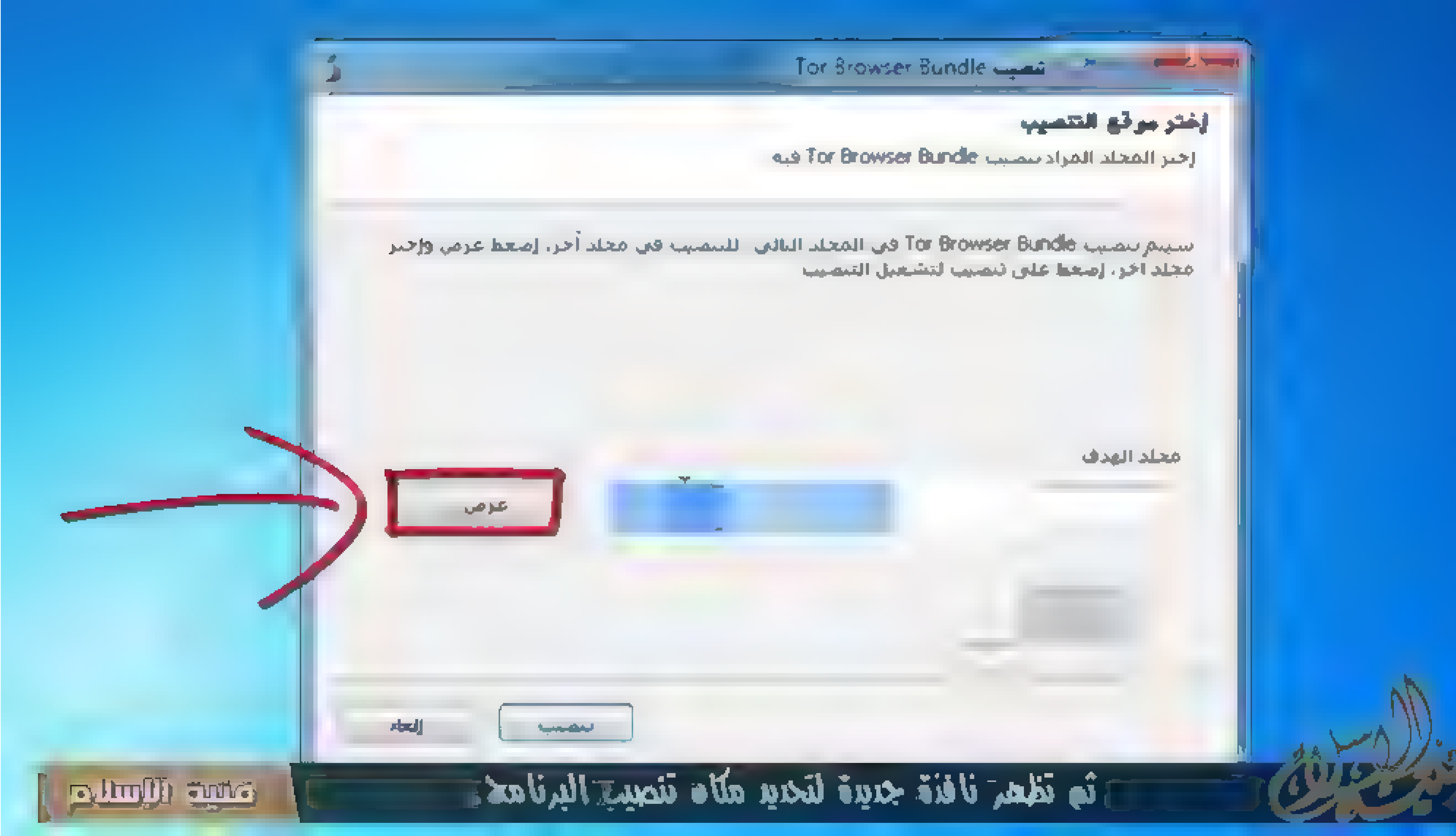


بعد إنتهاء تحميل البرنامج، يكون بالشكل التالي، نقوم بفتحه



تظهر لنا نافذة جديدة، نختار منها اللغة ونضغط موافق

فتية الإسلام


تنصيب Tor Browser Bundle
إختر موقع التنصيب
إختر المجلد المراد تنصيب Tor Browser Bundle فيه
سيتم تنصيب Tor Browser Bundle في المجلد التالي. للتنصيب في مجلد آخر، إضغط عرض واختر
مجلد آخر. إضغط على تنصيب لتشغيل التنصيب
مجلد الهدف
عرض
تنصيب
إلغاء
ثم تظهر نافذة جديدة لتحديد مكان تنصيب البرنامج



تنصيب Tor Browser Bundle
إختر موقع التنصيب
إختر المجلد المراد تنصيب Tor Browser Bundle فيه
سيتم تنصيب Tor Browser Bundle في المجلد التالي. للتنصيب في مجلد آخر، إضغط عرض واختر مجلد آخر. إضغط على تنصيب لتشغيل التنصيب
مجلد الهدف
عرض
تنصيب
إلغاء
وبعد تحديد مكان التنصيب نضغط زر تنصيب
منبر الإسلام





إنهاء مرشد إعداد Tor Browser Bundle

لقد تم تنصيب Tor Browser Bundle على الجهاز

إضغط إنهاء لإغلاق مرشد الإعداد

 شغل Tor Browser Bundle

إنهاء

وبعد إنتهاء التنصيب نضغط زر إنهاء



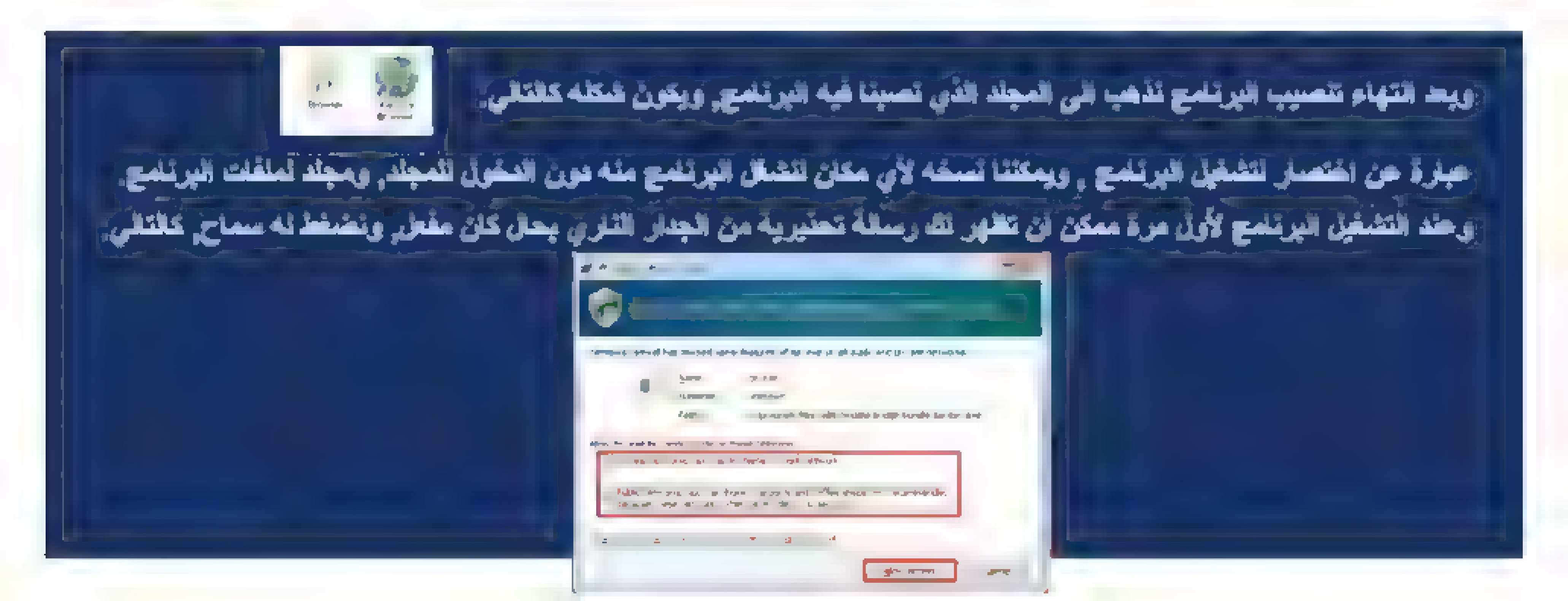
حِزم برنامج «تور» وكيفِية التعامل مع البرنامج :

وهي نسخة من برنامج «تور» إضافة إلى متصفح «فايرفوكس» تم تعديله من قبل مطورين لتوفير أمان أكبر للمتصفح مزود بمجموعة من الإضافات مختارة بعناية لتوفر أكبر قدر من الأمان، وهي

تحتوي هذه الإضافة قائمة لمئات المواقع التي تدعم التشفير حيث تجبر المتصفح على زيارة وتبادل البيانات في هذه المواقع باستخدام نسخة https.

تتيح هذه الإضافة خيارات واسعة للمستخدم للتحكم في المتصفح والإضافات والرموز «أكواد برمجية» للتقليل من المخاطر الناجمة عن الرموز والبرمجيات الخبيثة المدمجة بالصفحات.

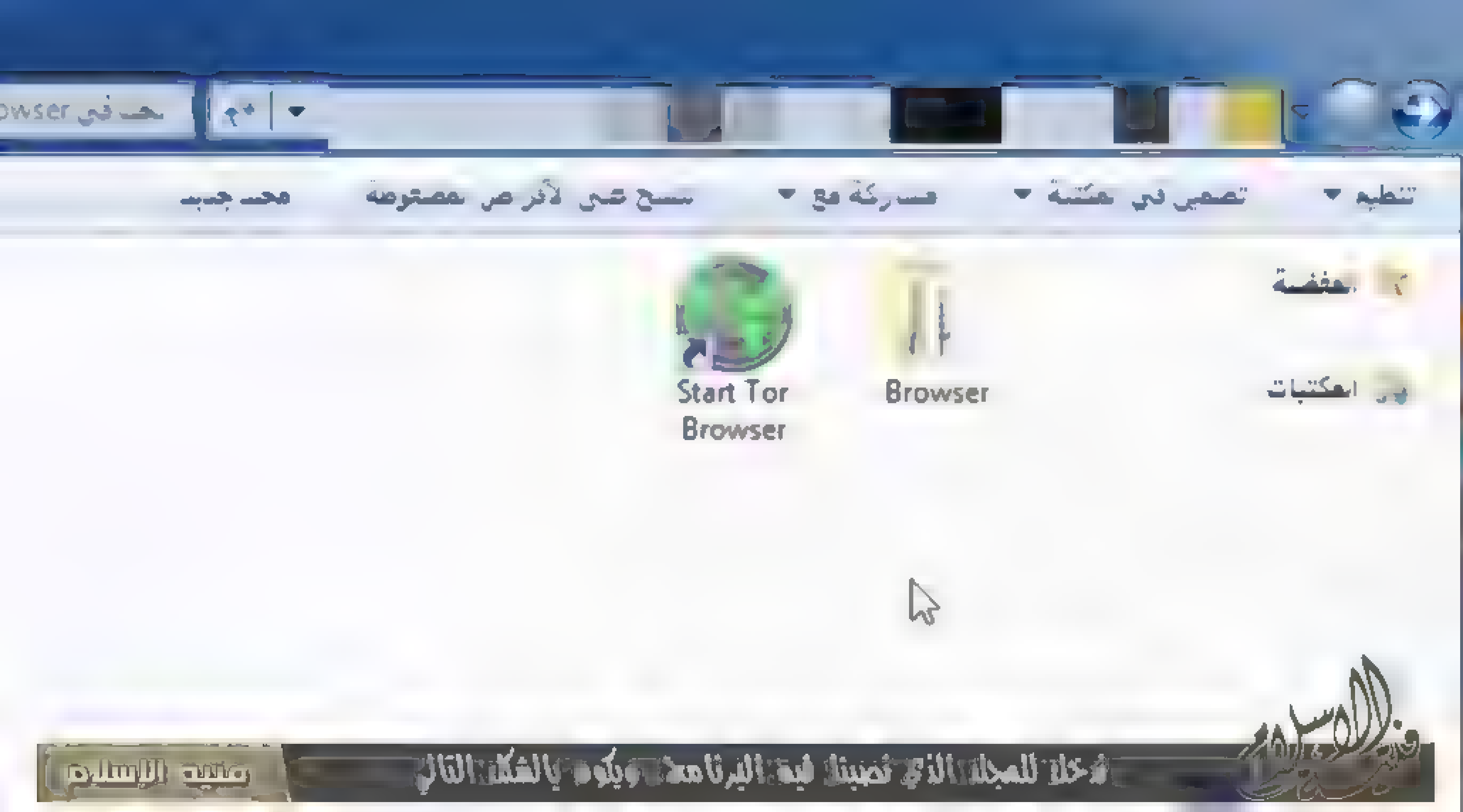
حزم برنامج «تور» وكيفية التعامل مع البرنامج :

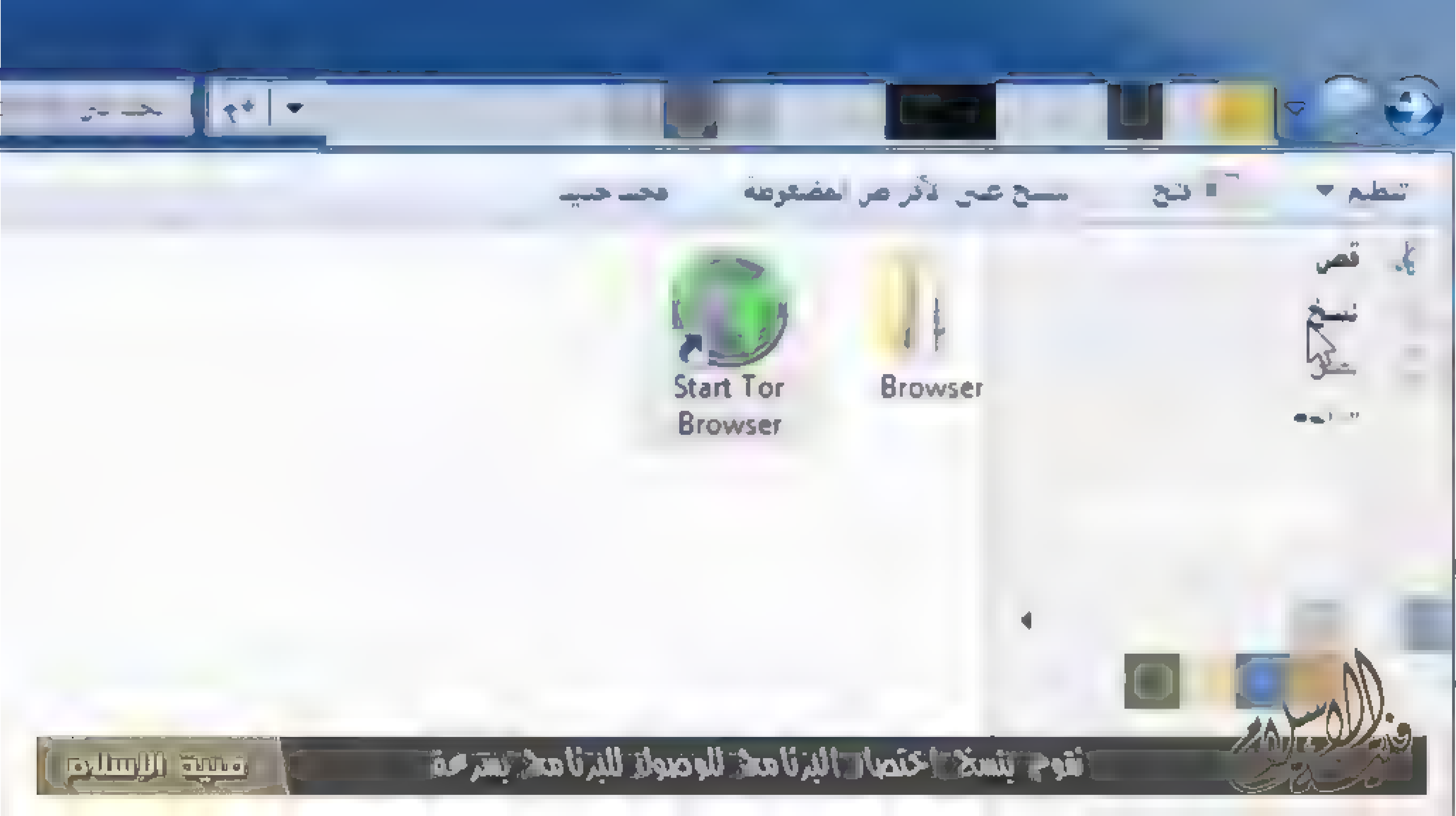




جزم برنامج «تور» وكيفية التعامل مع البرنامج :

دعونا نشاهد شرح بسيط لتشغيل البرنامج


Start Tor Browser
Browser

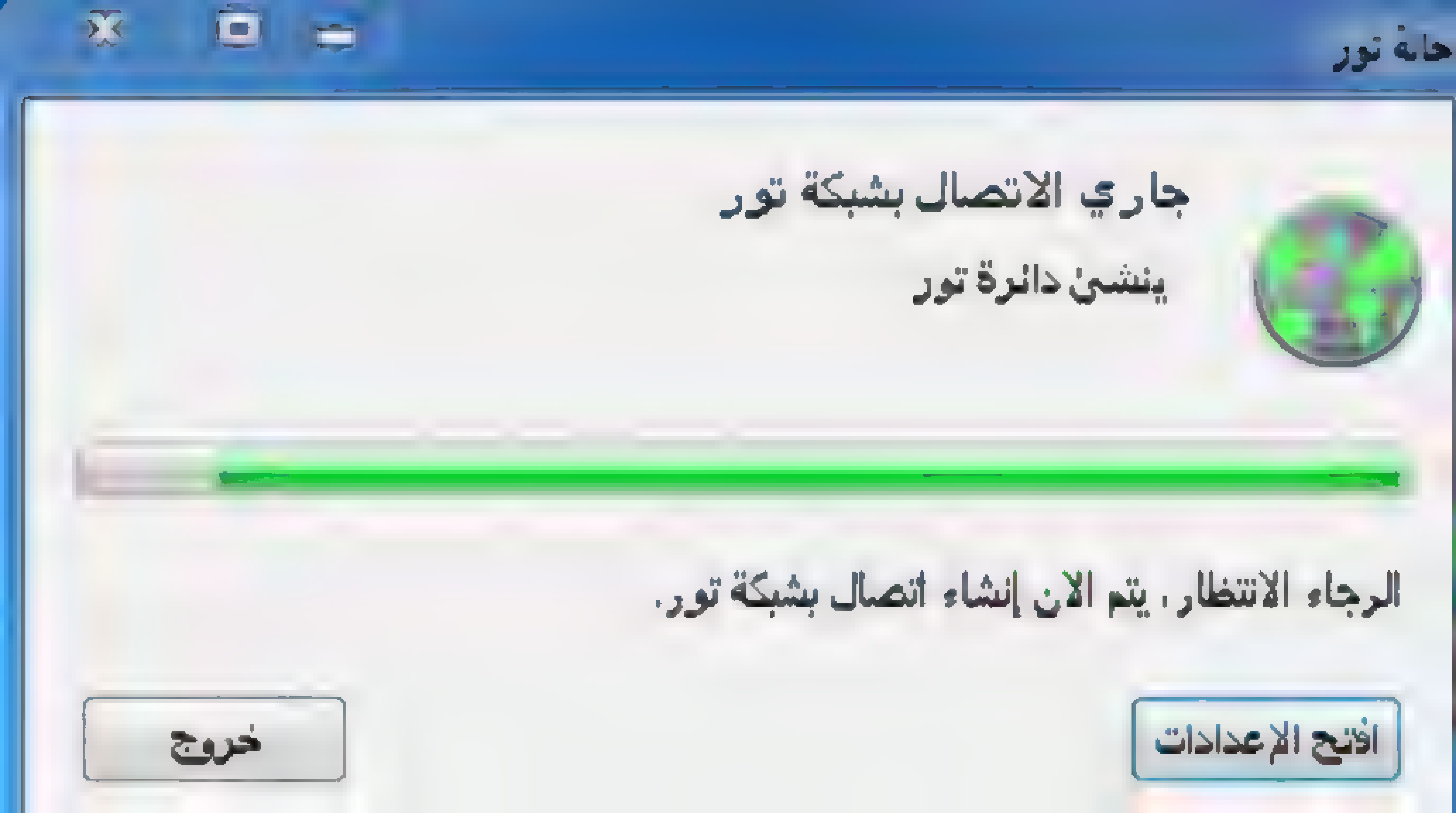

Start Tor
Browser
Browser
نقوم بنسخ اختصار البرنامج للوصول للبرنامج بسرعة



نُشغل البرنامج وننتظر ظهور نافذة الاتصال

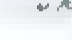
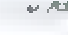
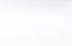


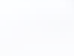
الإسلام



حالة تور
جاري الاتصال بشبكة تور
ينشئ دائرة تور
الرجاء الانتظار، يتم الآن إنشاء اتصال بشبكة تور.
افتح الإعدادات
خروج









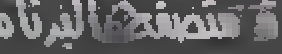
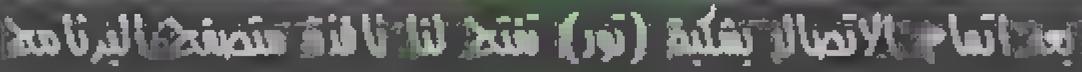
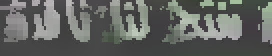
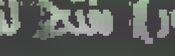
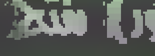



تهانينا!
هذا المتصفح معد لاستخدام شبكة تور



Startpage
ماذا بعد؟
يمكنك المساعدة!

فتية الإسلام






بعد اتمام الاتصال بشبكة (تور) تفتح لنا نافذة متصفح البرنامج



حِزم برنامج «تور» وكيفية التعامل مع البرنامج :

كيفية التعامل مع البرنامج وتجاوز الحظر [illegible]

وإن فشل الاتصال بشبكة «تور» وظهر لك رسالة أنه لا يمكن الاتصال فقد يكون البرنامج محظور في بلدك

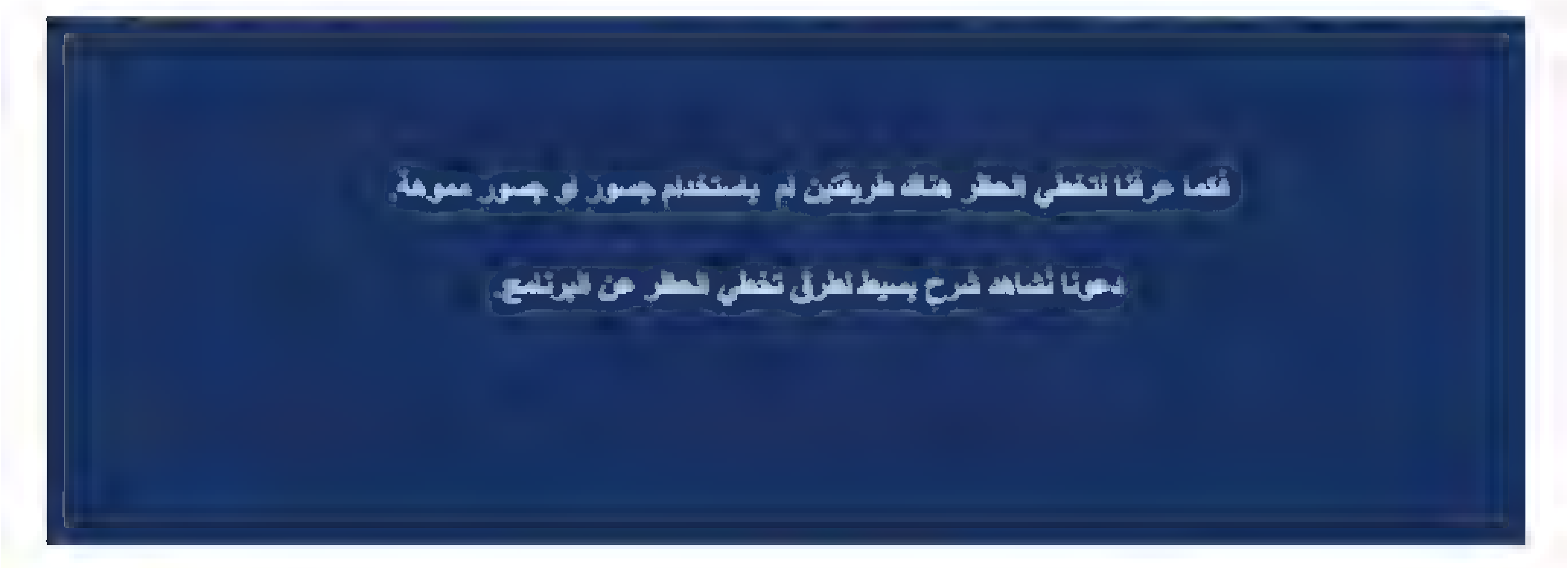
فالبرنامج أصبح محظور من قبل الكثير من حكومات الطواغيت كـ آل سعود وغيرهم.

ولتشغيل البرنامج بهذه الحالة علينا استخدام «الجسور» لتفادي الحظر على البرنامج.

«الجسور»: وهي عبارة عن «عقد تور» غير مدرجة في الدليل الرئيسي للبرنامج، وبالتالي لا يتصل «تور» بها تلقائيا، ما يجعل من غير الممكن لمزود خدمة الإنترنت معرفتها.

«الجسور المموهة»: عند الاتصال بـ «تور» يقوم البرنامج بإرسال بيانات في «ترويسة الاتصال» إلى مزود خدمة الإنترنت، وتشير بعض هذه البيانات إلى أن هذا الاتصال يتم بواسطة «تور». وتعمل الجسور المموهة باستخدام بروتوكول يسمى «obs3» مهمة هذا البروتوكول هو تمويه البيانات المرسلة كاملة لكي لا يعرف مزود الخدمة أنك تستخدم تور.

حزم برنامج «تور» وكيفية التعامل مع البرنامج :





عليك توفير معلومات حول اتصال هذا الحاسب بالإنترنت قبل أن تحاول الاتصال بشبكة تور

أي مما يلي يصف الأفضل لموقفك؟

أود الاتصال مباشرة إلى شبكة تور
سيصلح هذا في معظم الحالات

اتصل

اتصال هذا الحاسب بالإنترنت محجوب أو به بروكسي
على تكوين عدوات الجسر أو بروكسي

تكوين

للمساعدة اتصل بـ help@rt.torproject.org

نسخ سجل تور إلى الحافظة

التالي ›

خروج

نضغط على زر تكوين.

عقيدة الإسلام

حِزم برنامج «تور» وكيفية التعامل مع البرنامج :

شرح عن حزم برنامج «تور» وكيفية التعامل مع البرنامج

وهي نسخة تُستخدم لجعل جهازك كـ «عقدة» وتقوم بمساعدة المستخدمين حول العالم في تجاوز الرقابة والحجب وتأمين مجهولية الاتصال.

ولكن يجب الإشارة إلى أنه عليكم امتلاك سرعة إنترنت عالية لتوفير السرعة الكافية للمستخدمين حول العالم.

هذه الحزمة تمكنكم من تشغيل جهازكم كعقدة دخول أو عقدة منتصف.

وتأتي هذه الحزمة مع نسخة من برنامج «تور» فقط من دون المتصفح، إضافة إلى واجهة برنامج التي تتيح لكم الاتصال بشبكة تور وإعداد العقدة.

وهناك حزم أخرى تجعل جهازك عقدة الخروج أو جسر للمستخدمين الذين حُظر عنهم «تور» في بلدانهم من قبل الحكومات.



هل يحتاج هذا الجهاز إلى بروكسي حتى يصل إلى شبكة الإنترنت؟

- نعم
- لا

وإذا لم تكن متأكد من كيفية الإجابة على هذا السؤال، ألقي نظرة على إعدادات الإنترنت في متصفح آخر حتى تتأكد إذا كان يستخدم بروكسي

للمساعدة اتصل ب help@rt.torproject.org

انسخ سجل تور إلى الحافظة | < للخلف | التالي > | خروج

وعندما يسألنا عن استخدام البروكسي نضع الخيار (لا) ونضغط التالي



هل يقوم مقدم خدمة الإنترنت (ISP) الذي تتعامل معه بحجب الاتصالات بشبكة Tor أو مراقبتها بطريقة أخرى؟

نعم

لا

إذا لم تكن متأكد من إجابة هذا السؤال، قم باختيار لا. إذا قمت باختيار نعم، فسيطلب منك تكوين جسور Tor والتي هي مرحلات ترحيل غير مدرجة تصعب عملية حظر الاتصالات بشبكة Tor

للمساعدة اتصل بـ help@rt.torproject.org

نسخ سجل تور إلى الحافظة

< للخلف

التالي >

خروج

وعندما يسألنا هل مزود خدمتك يحجب (تور) نختار نعم ثم نضغط التالي

منبر الإسلام



يمكنك استخدام مجموعة الجسور المتوفرة أو الحصول على مجموعة مخصصة من الجسور

الاتصال بالجسور المتوفرة

نوع النقل obfs3 (موصى به)

مساعدة

إدخال جسور مخصصة

للمساعدة اتصل بـ help@rt.torproject.org

نسخ سجل تور إلى الحافظة

خروج

وهنا يوفر لك طريقتين للاتصال بشبكة تور بحال كان محظور

فتية الإسلام



يمكنك استخدام مجموعة الجسور المتوفرة أو الحصول على مجموعة مخصصة من الجسور

الاتصال بالجسور المتوفرة

نوع النقل obfs3 (موصى به)

مساعدة

إدخال جسور مخصصة

للمساعدة اتصل بـ help@rt.torproject.org

نسخ سجل تور إلى الحافظة | للخلف | اتصل | خروج

باختيار احدى الجسور المتوفرة من القائمة والضغط على زر اتصال

مكتبة الإسلام



يمكنك استخدام مجموعة الجسور المتوفرة أو الحصول على مجموعة مخصصة من الجسور

لاتصل بالجسور الموفرة

إدخال جسور مخصصة

أدخل جسر أو أكثر (جسر واحد في كل سطر)

مساعدة

للمساعدة اتصل بـ help@rt.torproject.org

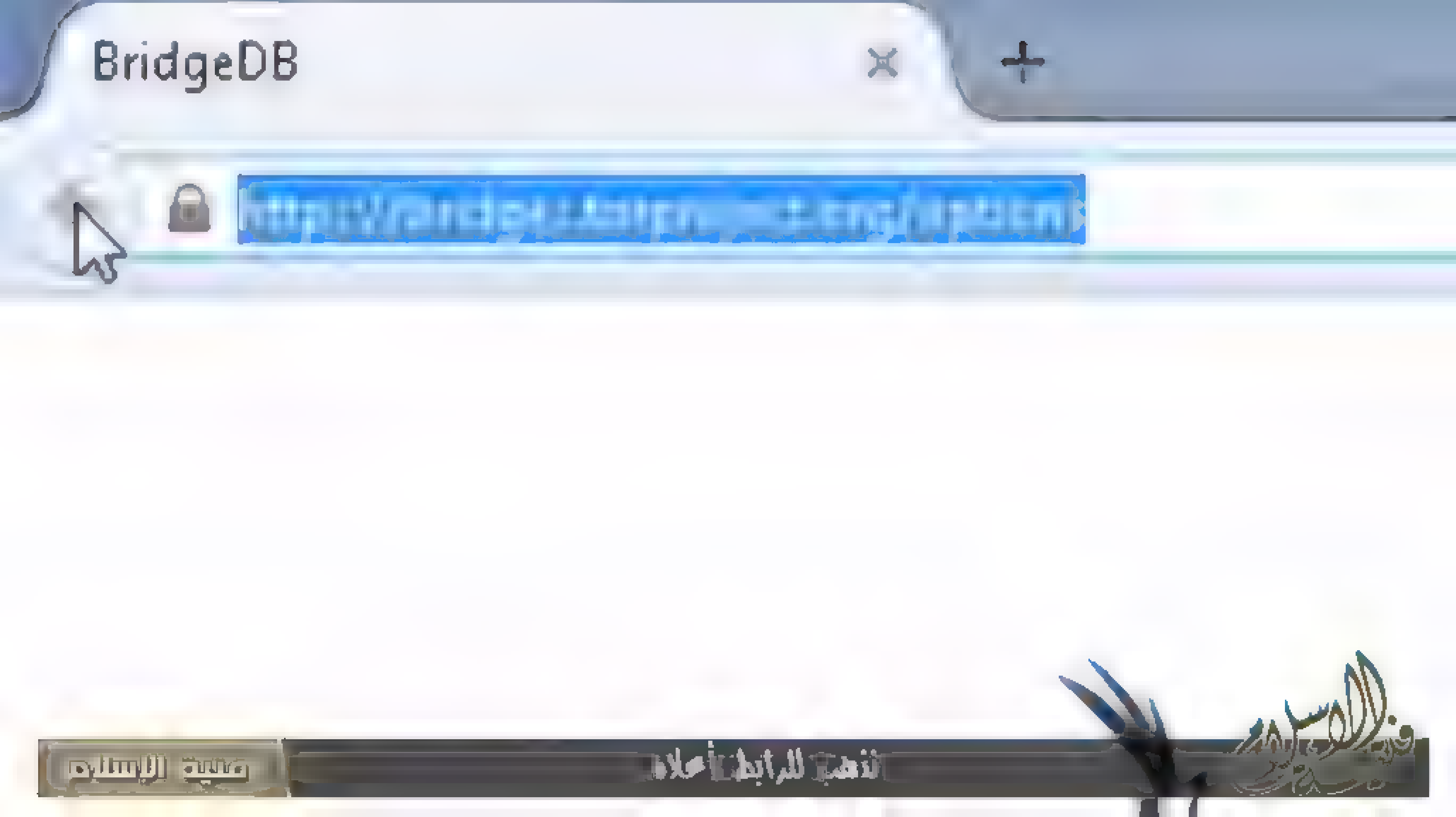
نسخ سجل تور إلى الحافظة

< للخلف

اتصل

خروج

٢- باختيار جسور أخرى بشكل يدوي ونجلبها من موقع البرنامج


BridgeDB



Get Bridges!

BridgeDB can provide bridges with several which can help obfuscate your connections to the Tor Network, making it more difficult for anyone watching your internet traffic to determine that you are using Tor.

Some bridges with IPv6 addresses are also available, though some Pluggable Transports aren't IPv6 compatible.

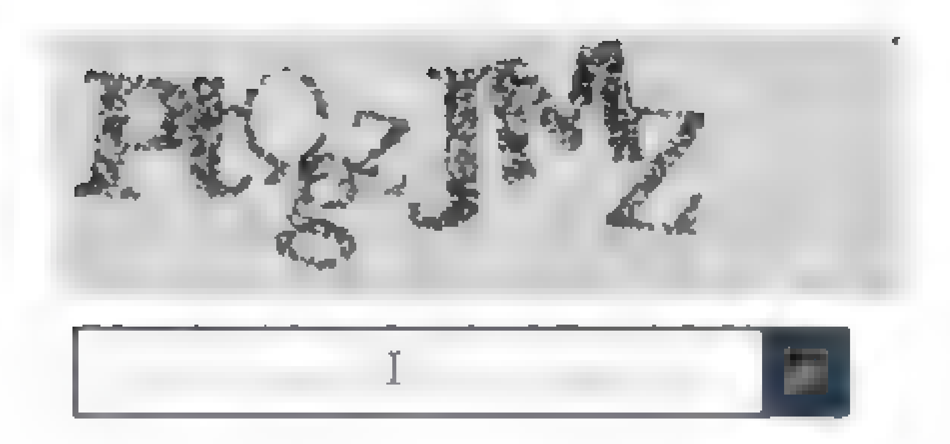
Additionally, BridgeDB has plenty of plain-ol'-vanilla bridges — without any Pluggable Transports — which maybe doesn't sound as cool, but they can still help to circumvent internet censorship in many cases.





ثم نضغط على زر (Just give me bridges)





What are bridges?

are Tor relays that help you circumvent censorship.





Another way to get bridges is to send an email to ... Please note that you must



Here are your bridge lines:

```
54.2[illegible]8.1[illegible]7.21[illegible]:44[illegible] d[illegible]
178.202.33.148:443 79a16bc40[illegible]
[illegible] 211.24[illegible].[illegible]18:4999 7[illegible]
```

How to start using your bridges

To enter bridges into Tor Browser, follow the instructions on the [illegible] download page to start Tor Browser. When the 'Tor Network Settings' dialogue pops up, click 'Configure' and follow the wizard until it asks:

Does your Internet [illegible] censor connections to the Tor network?









Here are your bridge lines:

[illegible]

[illegible]

[illegible]

How to start using your bridges

To enter bridges into Tor Browser, follow the instructions on the [illegible] to start Tor Browser. When the 'Tor Network Settings' dialogue pops up, click 'Configure' and follow the wizard until it asks:

Does your Internet Service Provider (ISP) block or otherwise censor connections to the Tor network?









حِزم برنامج «تور» وكيفية التعامل مع البرنامج :

طبعا سنتعامل مع الحزمة Tor Browser وهي الأفضل والأشمل وسنقوم بتحميلها من الموقع الرسمي من الرابط التالي:

https://www.torproject.org/download/download

فتظهر لنا عدة برامج نختار منها القائمة التي تمثل نظام تشغيلنا, فإن كنا نستخدم ويندوز بأي إصدار كان, فنختار Microsoft Windows

ثم نضغط على زر Download لنسخة Tor Browser

وبحال كان موقع البرنامج محظور ببلدك, فعليك تحميله من الرابط البديل التالي:

http://download.cnet.com/Tor-Browser-Bundle/3000-2356_4-75660251.html

torproject.org

Here are your bridge lines:

54 230 167.213 443 d732[illegible]

178 202 33 140 443 79a16bc4037c3995[illegible]



يمكنك استخدام مجموعة الجسور المتوفرة أو الحصول على مجموعة مخصصة من الجسور

لاتصل بالجسور المتوفرة

● إستعمل جسور مخصصة

مساعدة

ادخل جسر أو أكثر (جسر واحد في كل سطر)

[illegible] 443

79a16bc4037c39951e0b4b55bb2b0b [illegible] 178 202 33 140 443

7cdce [illegible] 93 211 243 218 34999

للمساعدة، اتصل بـ help@rt.torproject.org

خروج | اتصل | رجوع

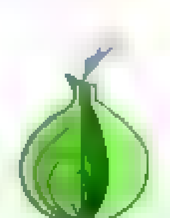
To enter bridges into Tor Browser, follow the instructions on the [illegible] to start Tor Browser. When the Tor Network Settings dialogue pops up, click Configure and follow the wizard until it asks









تهانينا!

هذا المتصفح معد لاستخدام شبكة تور

أنت الآن حر في تصفح شبكة الإنترنت بشكل مجهول



ماذا بعد؟

يمكنك المساعدة!



وإن شاء الله سيتم عملية الاتصال بنجاح

تقنية الإسلام



جزم برنامج «تور» وكيفية التعامل مع البرنامج :

فلذا اخترت الاتصال بالجسور المتوفرة فكل ما عليك هو الاختيار من القائمة ويفضل اختيار obfs3 ثم اضغط زر اتصال.

اما اذا اخترت الجسور المخصصة وهو الأفضل فعليك جلب جسور من الرابط التالي واضفتها بشكل يدوي.

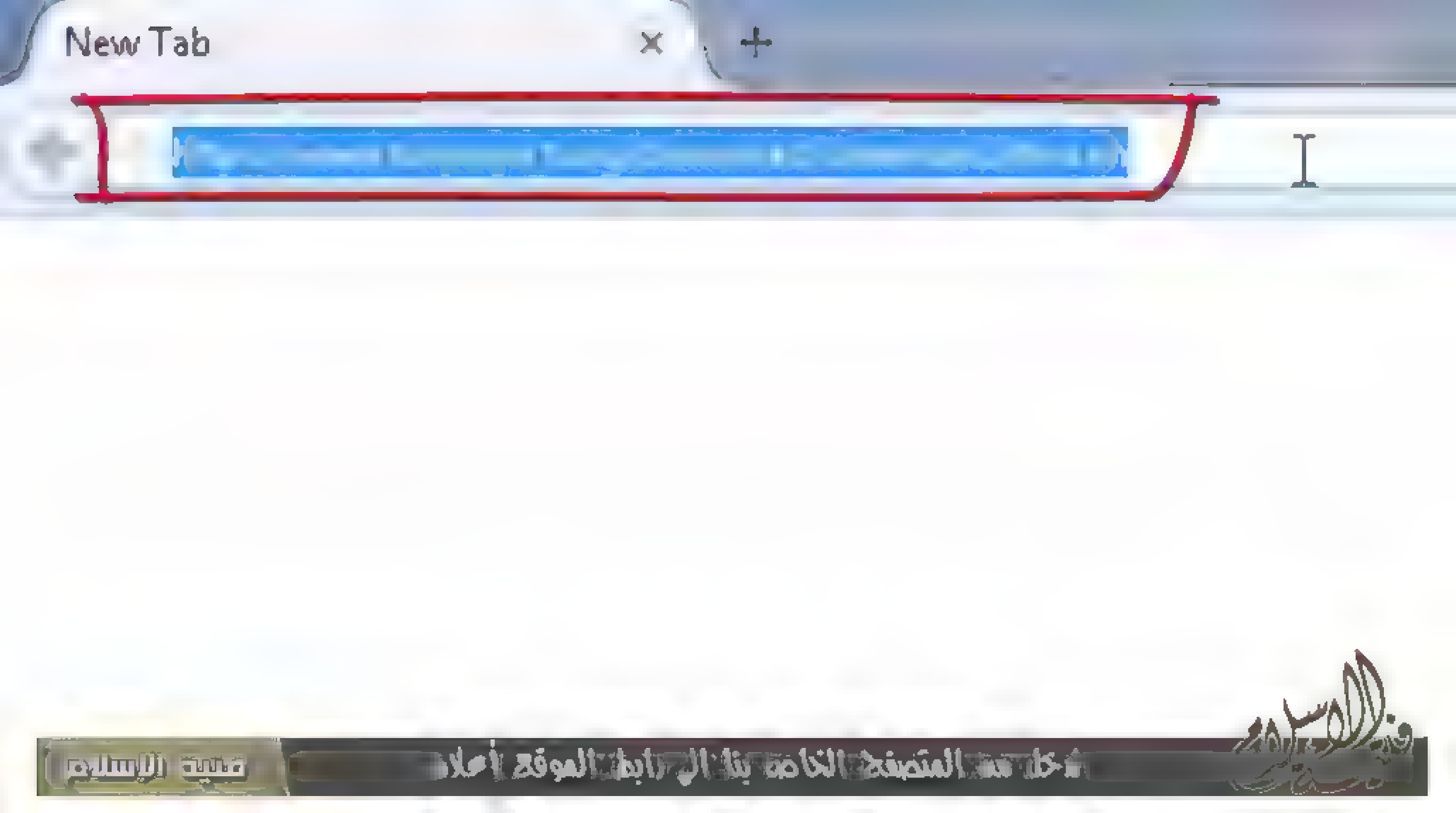
https://bridges.torproject.org/options

حزم برنامج «تور» وكيفية التعامل مع البرنامج :

بعد الاتصال بشبكة «تور» يمكنك اخذ هوية جديدة من «تور» بأي وقت أردت
ما عليك سوى الضغط على رمز «البصلة» في المتصفح ثم اضغط على «هوية جديدة»، وبعدها سيتم تنظيف المتصفح
واعطائك هوية جديدة و «ip» جديد وننصح دائماً بطلب هوية جديدة بحالة تشنج المتصفح أو الحظر من موقع ما.

حِزم برنامج «تور» وكيفية التعامل مع البرنامج :




New Tab

HOME › DOWNLOAD

Want Tor to really work?

You need to change some of your habits, as some things won't work exactly as you are used to. Please read the [illegible] for details

Microsoft Windows

Apple OS X

GNU/Linux, BSD, and Unix

Tor for Smartphones

Source Code

Expand All

Want Tor to really work?





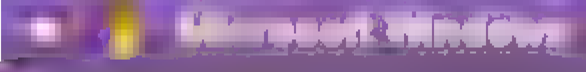
a. Use the Tor Browser

HOME » DOWNLOAD



Want Tor to really work?

You need to change some of your habits, as some things won't work exactly as you are used to. Please read the full list of warnings for details





Tor Browser

Version 4.0
Windows 8, 7, Vista

English

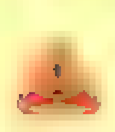
العربية
Deutsch
Español
فارسی
Français
Nederlands

Everything you need to safely browse the Internet



نختار لغة البرنامج التي تناسبنا

HOME » DOWNLOAD



Want Tor to really work?

You need to change some of your habits, as some things won't work exactly as you are used to. Please read the full list of warnings for details





Tor Browser

Version 4.0 - Windows 8, 7, Vista, and XP

Everything you need to safely browse the internet. Learn more »









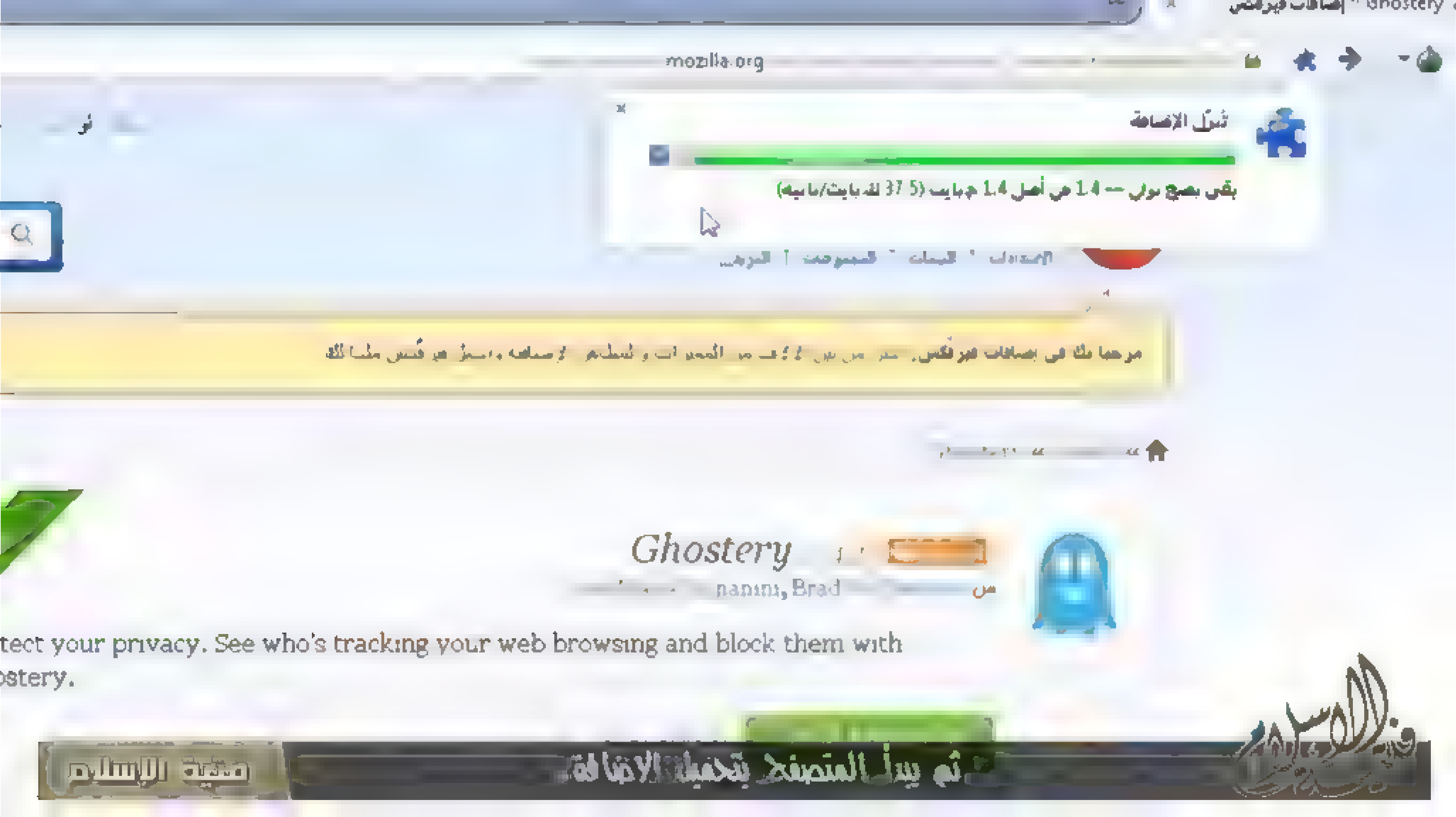
دورة التخفي والتصفح الآمن للإنترنت.

الدرس الثالث.

1- تعريف اضافات المتصفح

2- شرح تثبيت الإضافات على المتصفح

3- حل مشكلة إضافة الخصوصيه بحظر بعض الأدوات في المواقع



mozilla.org
تنزيل الإضافة
يبقى بضع ثوانٍ — 1.4 من أصل 1.4 ميجابايت (37.5 كيلوبايت/ثانية)
Ghostery
tect your privacy. See who's tracking your web browsing and block them with
ostery.
ثم يبدأ المتصفح بتحميل الإضافة



تثبيت البرمجيات
لا تثبّت إلا الإضافات الصادرة عن المؤلفين الذين تثق بهم.
يمكن للبرمجيات الخبيثة أن تضرّ بالحاسوب أو تنتهك خصوصيتك.
طلبت تثبيت العنصر التالي
Ghostery (Ghostery, Inc.)
mozilla.org/firefox/downloads/latest/9609/addon-9609-latest.xpi?src=dp-btn-primary
Ghostery
with

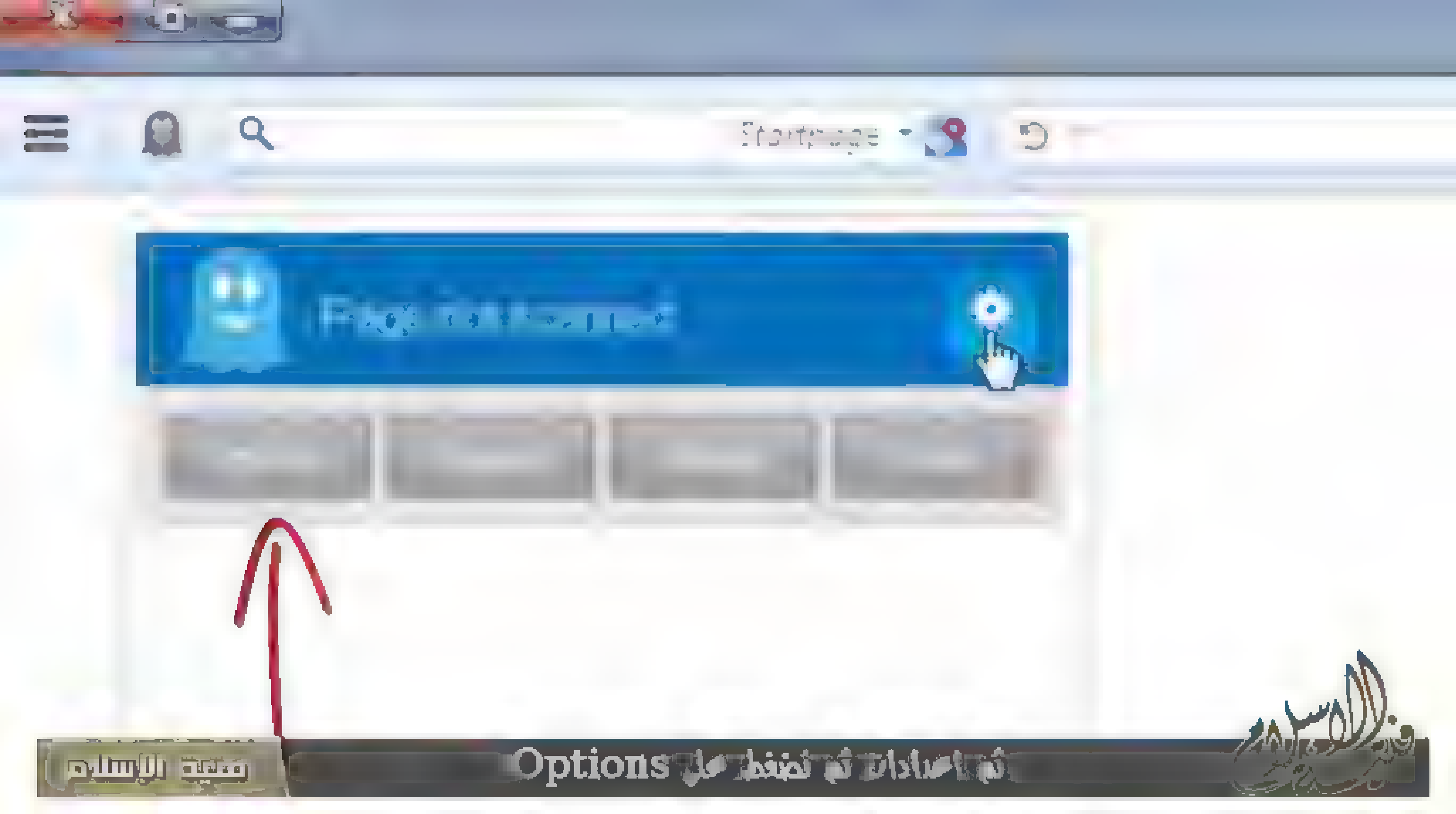
إضافات لمتصفح «تور» لخصوصية وأمان أعلى:





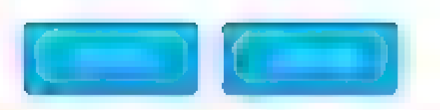
Startpage

اضغط على أيقونة الاضافة


Startpage
ثم اعدادات ثم تضغط على Options

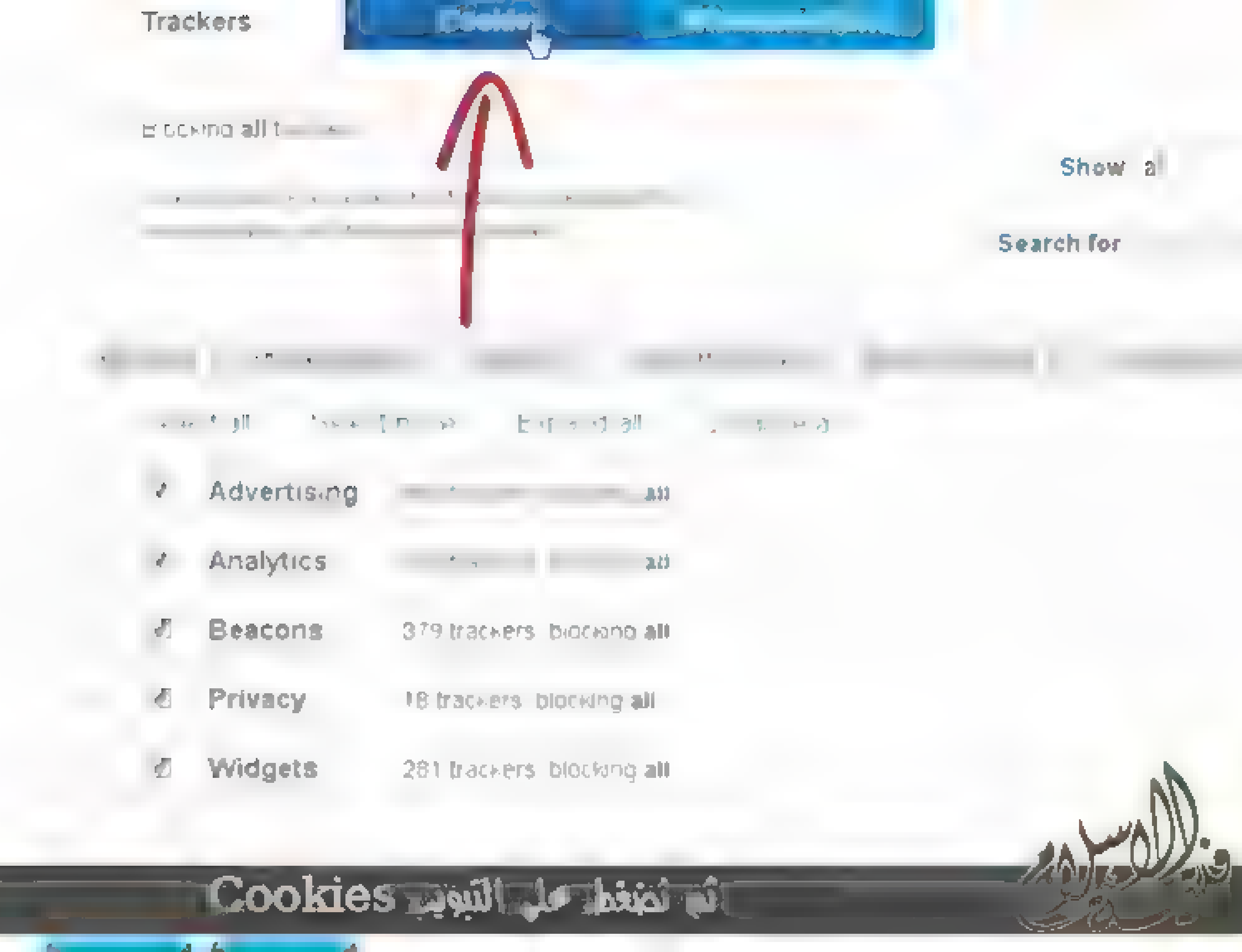
Search for

Advertis ng		none
Analytics		none
Beacons	379 trackers blocking	none
Privacy		none
W dgets		none



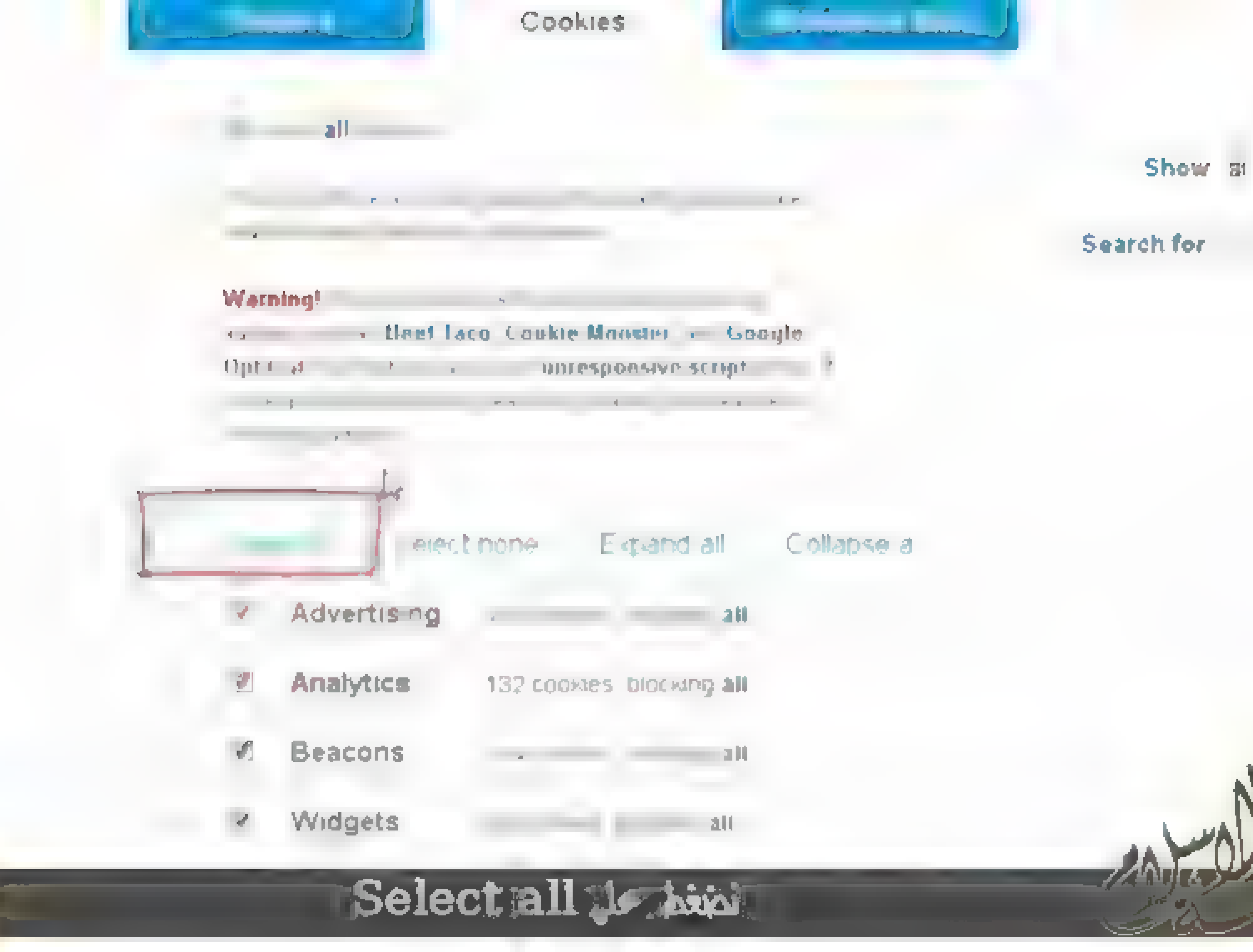
Select all انزل الى أسفل الصفحة واضغط على



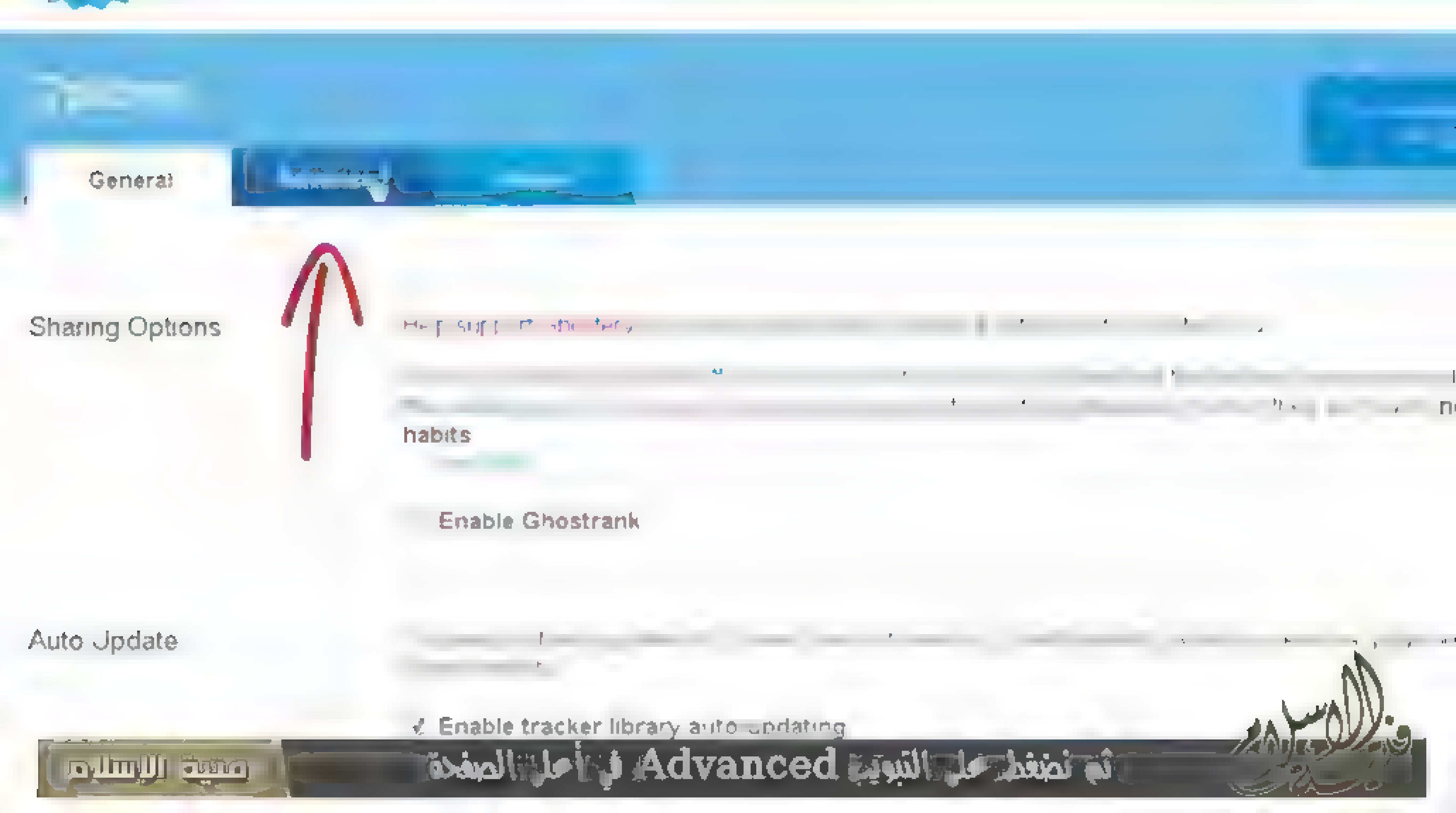


ثم تضغط على التبويب Cookies

منبر الإسلام



Cookies
Show
Search for
Warning!
unresponsive script
elect none
Expand all
Advertising
all
Analytics
132 cookies blocking all
Beacons
all
Widgets
all
Select all


General
Sharing Options
habits
Enable Ghostrank
Auto Update
Enable tracker library auto updating
ثم تضغط على التبويبة Advanced في أعلى الصفحة

Display Options

Show alert bubble

Reveal tracker source URL lists by default

✓ Show [illegible] tery's butt

Not ready for the new panel? Revert to the old menu temporarily (restart required)

Check to re-add Ghosty to Navigation Toolbar

Blocking Options

Ignore first party trackers [illegible] ick tracker on doubleclic

Auto Update

✓ Block new elements by default

Notify me of new elements

Click-to-Play

✓ Replace certain blocked content with a 'click-to-play' overlay

This helps when blocking potentially useful widgets such as video players, comm[illegible] forms.



إضافات لمتصفح «تور» لخصوصية وأمان أعلى:

الإضافات : هي أدوات نضيفها لمتصفح «تور» لأمور عدة، ولكل إضافة من هذه الإضافات عمل مخصص تقوم به.

وهي إضافات مخصصة لتأمين خصوصية وحماية أعلى للمستخدم، وأبرزها:

Ghostery

وهي إضافة قوية جداً للحماية والتحكم بالخصوصية وتقوم بمنع الكثير من الإضافات والإعلانات في المواقع.

رابط الإضافة : https://addons.mozilla.org/en-US/firefox/addon/ghostery/

وهي إضافة تقوم بإيقاف ومنع أي موقع من التجسس عليك و تتبع نشاطك دون موافقتك.

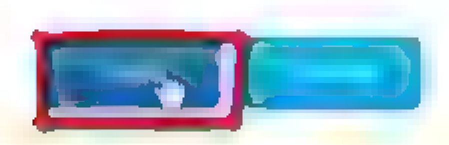
رابط الإضافة : https://addons.mozilla.org/en-US/firefox/addon/privacy-badger-firefox/

Language — ghostery in English

Import/Export

Performance Options

- ✓ Scan and block images
- ✓ Scan and block iframes
- ✓ Scan and block embed and object tags
- ✓ Look for and prevent redirection
- ✓ Delete Flash and Silverlight cookies on exit





ثم تضغط على Save



إضافات لمتصفح «تور» لخصوصية وأمان أعلى:



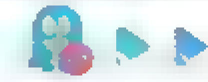






مثال على الأدوات التي تحظرها الاضافة

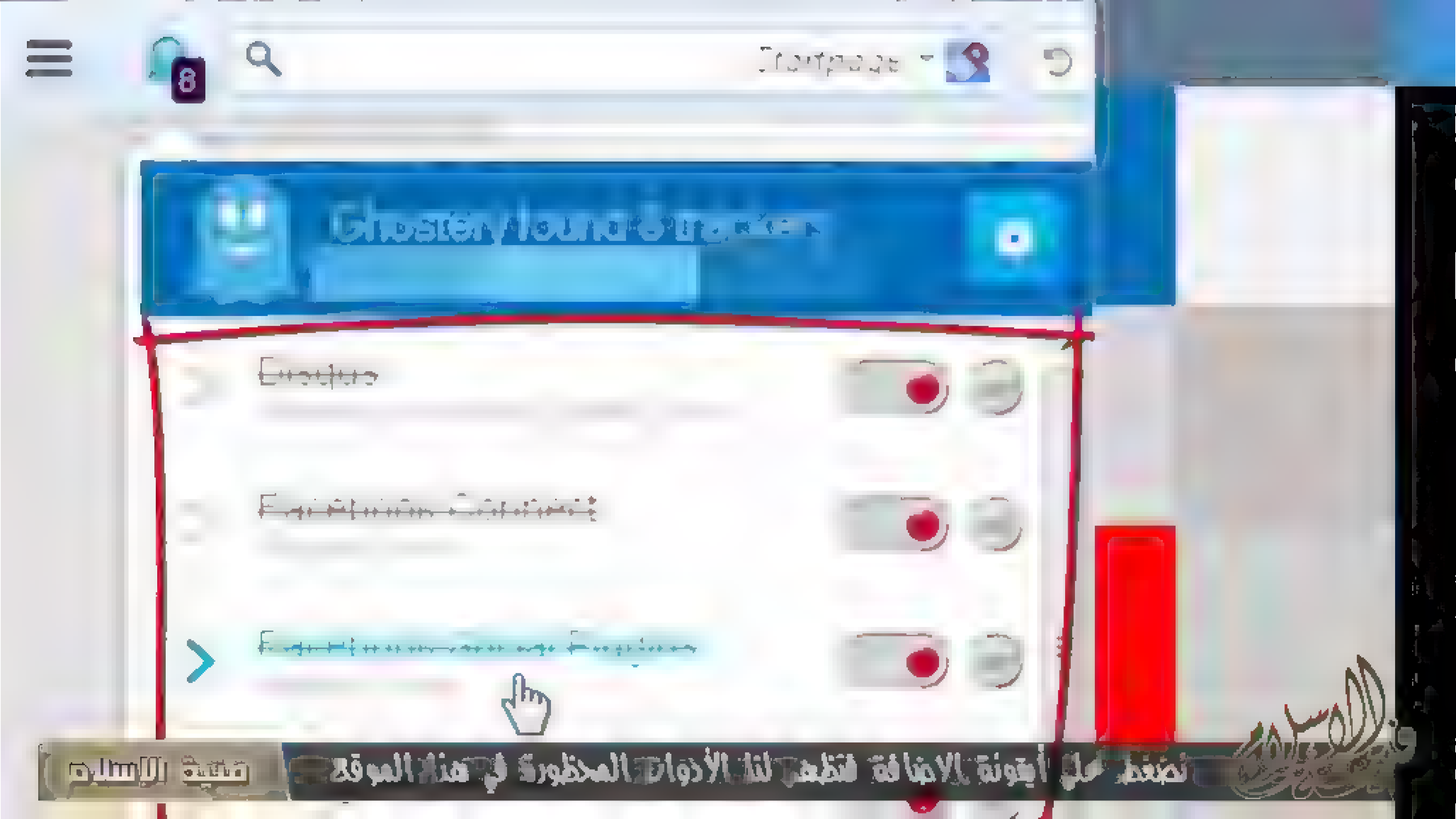
Ghostery blocked comments powered by Disqus

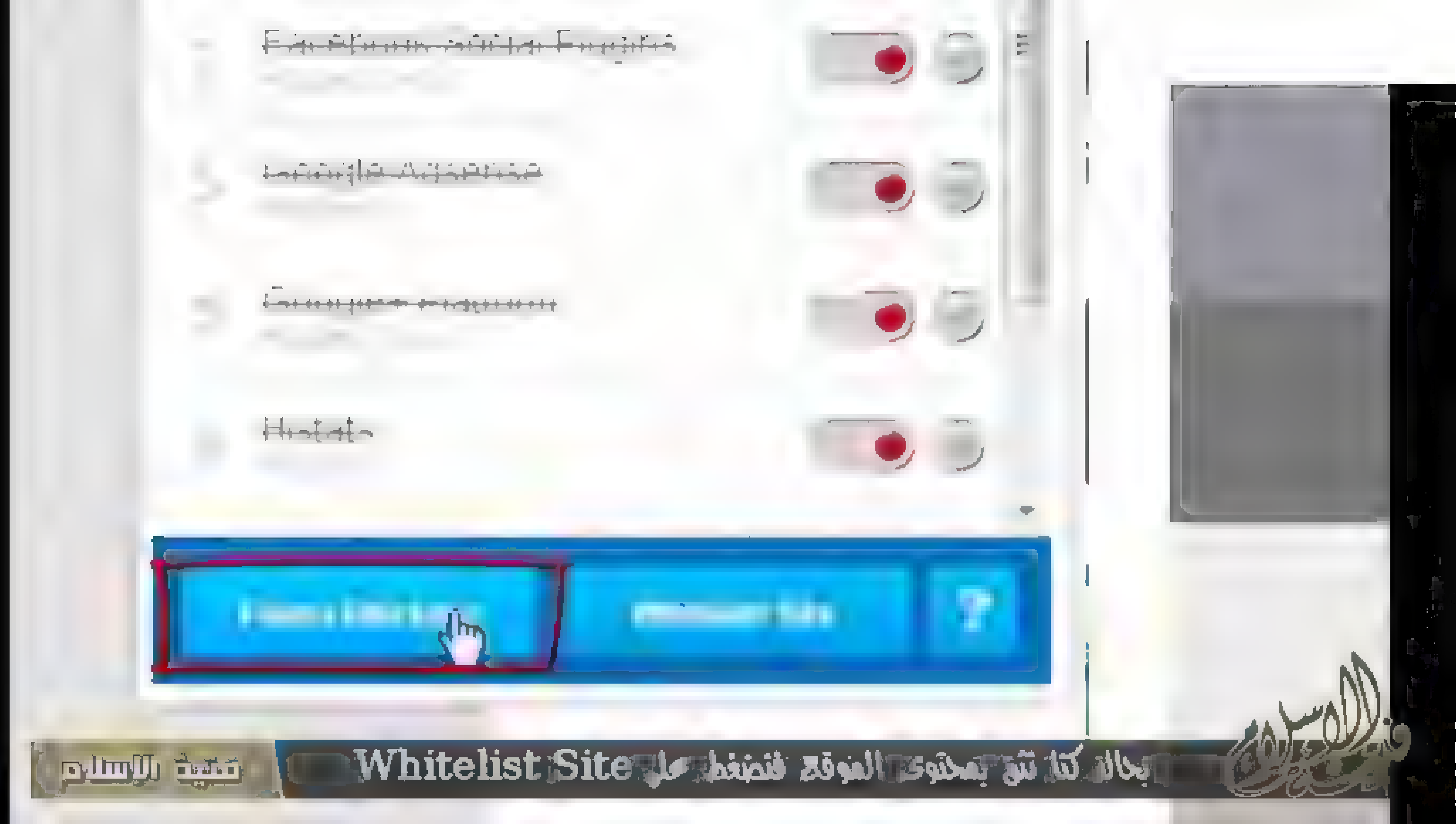




مثال على الأدوات التي تحظرها الإضافة



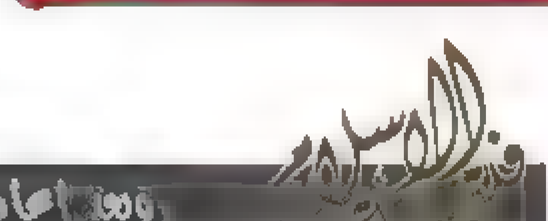

نضغط على أيقونة الإضافة فتظهر لنا الأدوات المحظورة في هذا الموقع
فتية الإسلام


بحال كنا نثق بمحتوى الموقع فنضغط على Whitelist Site
فتية الإسلام

Blocking is paused

اما بغير ذلك لنضغط على Pause Block ايقافا موقتا للحماية

Like 144 people like this ... to see what your friends like



ومع اعادة تحميل الصفحة نلاحظ ظهور الإعلانات وعمل الأدوات

إضافات لمتصفح «تور» لخصوصية وأمان أعلى:

وهكذا يتم حل المشكلة إما بإيقاف مؤقت للحماية بشكل كلي، أو إضافة الموقع إلى اللائحة البيضاء بحال كان موثوق المحتوى.

وبحال إضافة موقع ما إلى اللائحة البيضاء فإن الإضافة لن تقوم بعدها بحجب أي إضافة بداخل هذا الموقع.

ولا ننصح بإضافة الموقع إلى اللائحة البيضاء إلا بحالة كنت واثقاً تماماً من محتواه.

فئة الإسلام

إضافات لمتصفح «تور» لخصوصية وأمان أعلى:

وهي إضافة تُستخدم لجعل IP الخاص بك لبلد معين وإخفاء الأصلي،
طبعا «التور» يقوم بتغير IP الخاص بك كل بضعة دقائق، وهذا أفضل
لكن لماذا طرحت هذه الإضافة إذاً التي ستجعل IP الخاص بي ثابت في بلد معين في وقت التصفح؟

الإجابة هي أن بعض يدخل إلى بعض المواقع أو المنتديات التي تستخدم خدمة CloudeFlare وهي لصد الهجمات على الموقع

وهذه الخدمة عندما ترى ip الخاص بك من «تور» فإنها ستعتقد أنه هجومي
لذلك ستعرض لك رسالة لإدخال رمز تأكيد أنك شخص وليس روبوت



إضافات لمتصفح «تور» لخصوصية وأمان أعلى:

AnonymoX

وبعد إدخال رمز التأكيد بشكل صحيح سيتم إدخالك للصفحة المطلوبة، وعند دخول أي صفحة في الموقع سيطلب منك إدخال رمز،

لأن «التور» يقوم بتغير ip بشكل دائم، لذلك من تزعجه هذه الرسالة عند دخول الموقع أو المنتديات فعليه بستخدام هذه الإضافة

رابط الإضافة : https://addons.mozilla.org/ar/firefox/addon/anonymox/

مثال على رسالة التأكيد :

One more step



إضافات لمتصفح «تور» لخصوصية وأمان أعلى:

هناك بعض الإضافات التي سنضيفها لمتصفح «تور» لأمور عدة وأبرزها:

وهي إضافات تقوم بأعمال متنوعة، وأبرزها:

Adblock Plus

وهي إضافة تمنع ظهور الإعلانات على متصفحك.

رابط الإضافة : https://addons.mozilla.org/ar/firefox/addon/adblock-plus/

وهناك الكثير من الإضافات التي لا يسعنا ذكرها، وهذا رابط لأهم إضافات الخصوصية الأخرى:

http://adjustyourprivacy.com/privacy-tools/

فتية الإسلام

إضافات لمتصفح «تور» لخصوصية وأمان أعلى:

كل ما علينا هو الدخول إلى رابط الإضافة ثم الضغط على إضافة إلى فايرفوكس

ثم تظهر لنا رسالة نضغط سماح ثم ننتظر انتهاء التحميل ثم نضغط تنصيب

ونفس الطريقة لكل الإضافات وبعد الانتهاء من التنصيب نعيد تشغيل المتصفح
سنُنصب إضافة واحدة فقط وأنت أكمل الباقي بنفس الطريقة.

دعونا نشاهد شرح بسيط لطريقة تنصيب الإضافات للمتصفح


Ghostery :: إضافات فَيَرفُكس
الإضافات



Ghostery
الإضافات
Ghostery 5.4.1
Protect your privacy. See who's tracking your web browsing and block them with Ghostery.
ثم تضغط على Add to فايرفوكس



Ghostery :: إضافات فَيَرفُكس
mozilla.org
Ghostery
Protect your privacy. See who's tracking your web browsing and block them with Ghostery.



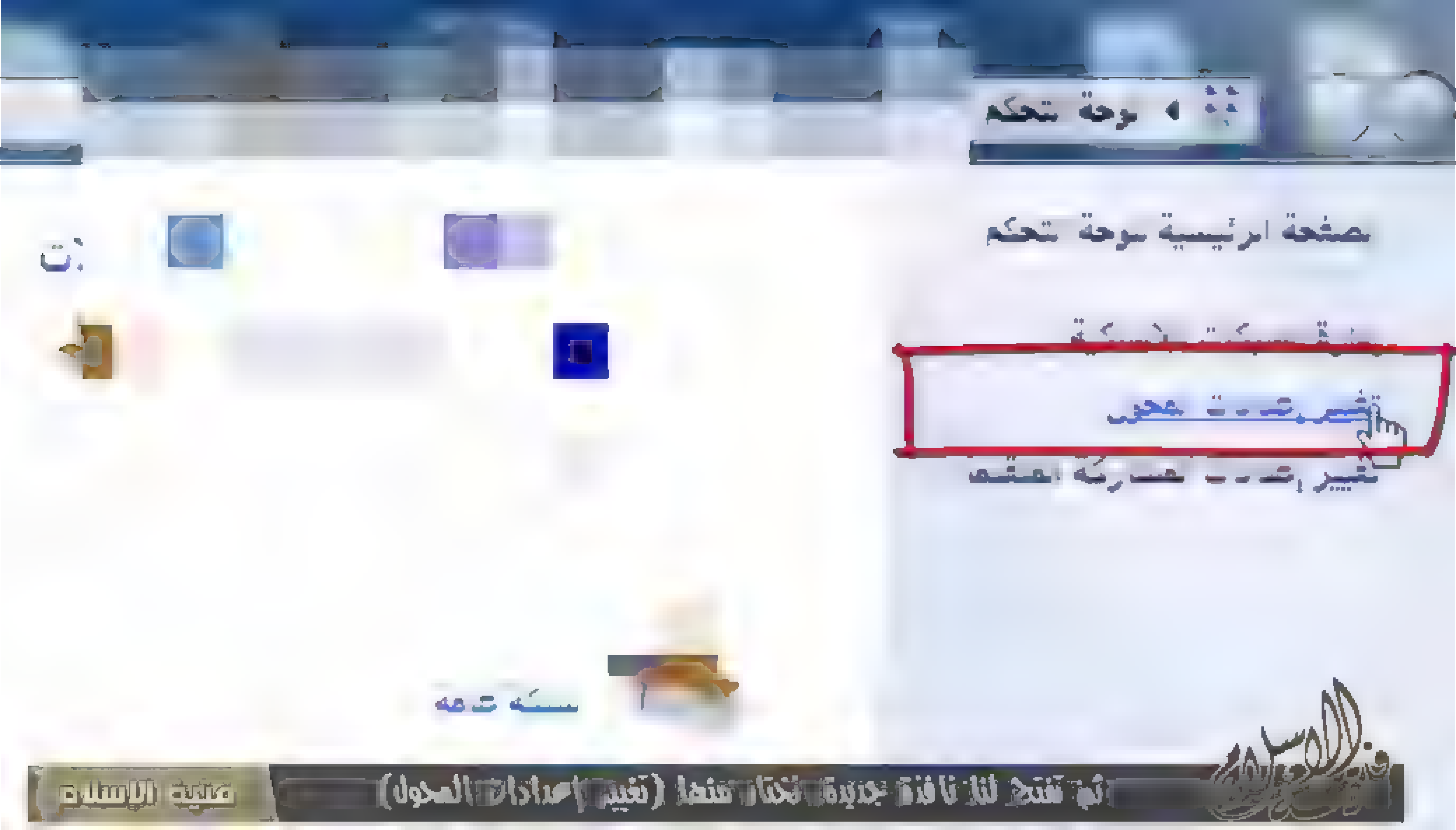
دورة التخفي والتصفح الآمن للإنترنت.

الدرس الرابع.

1- ما هو الـ DNS وطريقة عمله

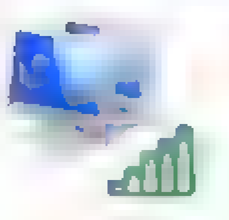
2- فحص تسريب الخوادم ومعرفة خطورة الأمر

3- تغيير الخوادم بشكل يدوي او عن طريق برامج



لوحة التحكم
صفحة الرئيسية لوحة التحكم
ثم تفتح لنا نافذة جديدة نختار منها (تغيير إعدادات المحول)

Wireless Network Connection

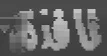




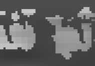


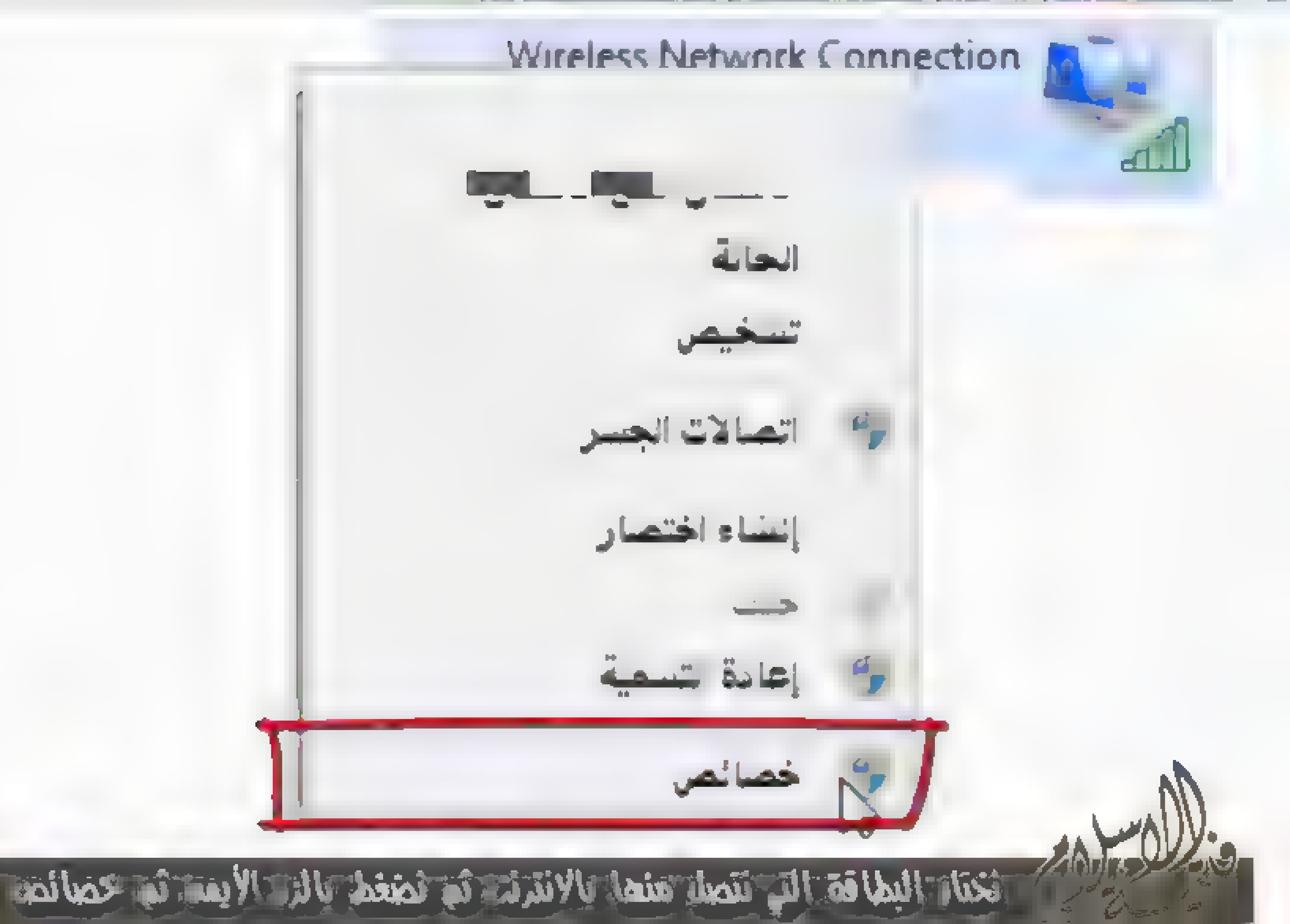


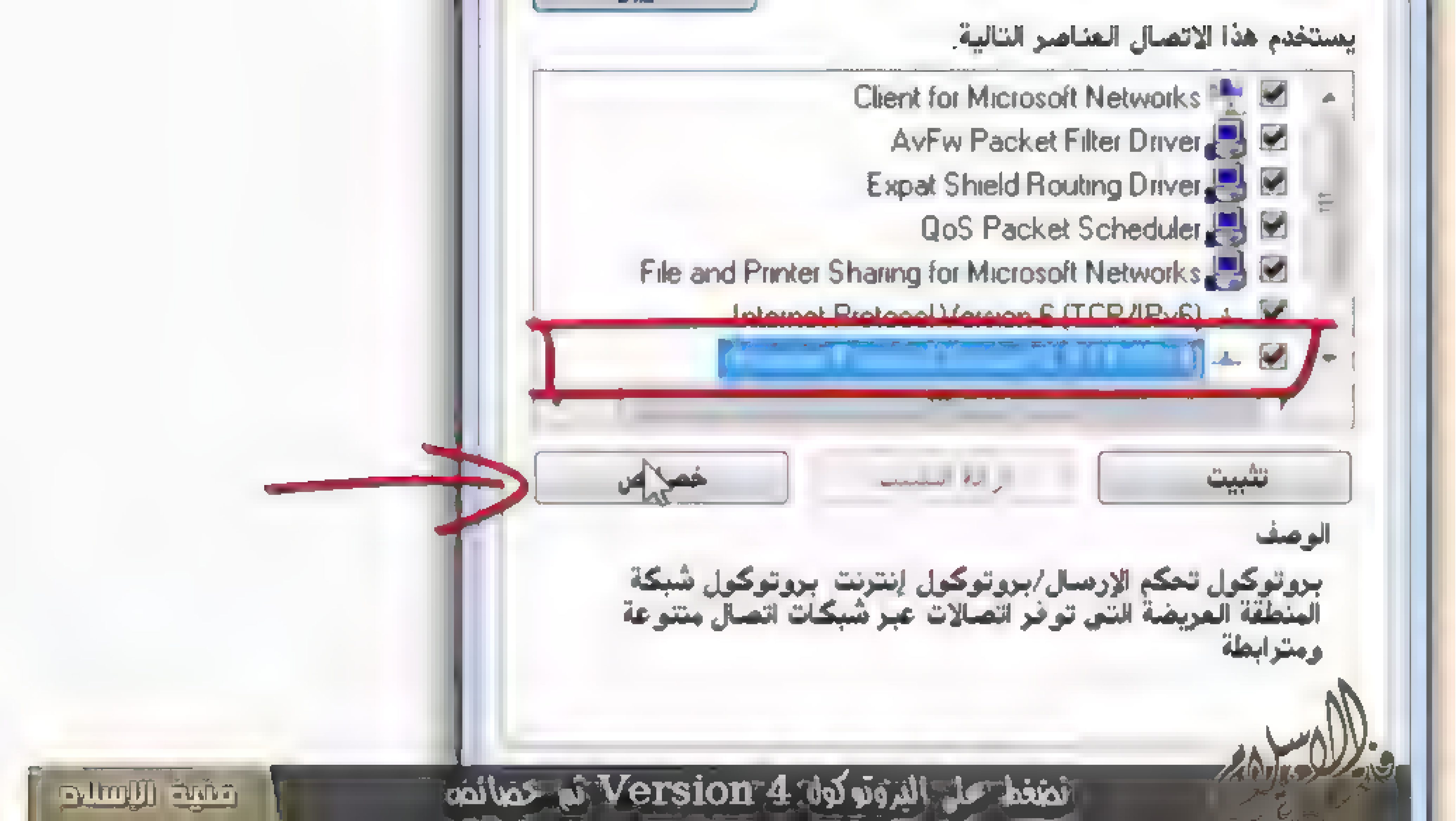









Wireless Network Connection
الحالة
تشخيص
اتصالات الجسر
إنشاء اختصار
إعادة تسمية
خصائص
نختار البطاقة التي نتصل منها بالانترنت ثم نضغط بالزر الأيمن ثم خصائص
فتية الإسلام



يستخدم هذا الاتصال العناصر التالية:
Client for Microsoft Networks
AvFw Packet Filter Driver
Expat Shield Routing Driver
QoS Packet Scheduler
File and Printer Sharing for Microsoft Networks
خصائص
تثبيت
الوصف
بروتوكول تحكم الإرسال/بروتوكول إنترنت بروتوكول شبكة المنطقة العريضة التي توفر اتصالات عبر شبكات اتصال متنوعة ومترابطة
نضغط على البروتوكول Version 4 ثم خصائص
منبر الإسلام

يمكنك الحصول على إعدادات IP المعينة تلقائياً إذا كانت الشبكة تعتمد هذه الإمكانية ولا ستحتاج لطلب إعدادات IP المناسبة من مسؤول الشبكة

الحصول على عنوان IP تلقائياً

استخدام عنوان IP التالي

الحصول على عنوان خادم DNS تلقائياً

استخدام عناوين خادم DNS التالية

خادم DNS المفضّل

خادم DNS البديل

ثم نختار الخيار (استخدام عناوين خادم Dns التالية)

يمكنك الحصول على إعدادات IP المعينة تلقائياً إذا كانت الشبكة تعتمد هذه الإمكانية. وإلا ستحتاج لطلب إعدادات IP المناسبة من مسؤول الشبكة

- الحصول على عنوان IP تلقائياً
- استخدام عنوان IP التالي

- الحصول على عنوان خادم DNS تلقائياً
- استخدام عناوين خادم DNS التالية:

خادم DNS المفضّل: 8 . 8 . 8 . 8

خادم DNS البديل:

ثم نضع الخوادم التي نريدها لا نتقيد بجهة أو خوادم نريدها

New Tab

http://dnsleaktest.com/

ثم تذهب إلى المتصفح لفحص التسريب من الرابط أعلاه

Hello



Standard test Extended test



ثم تضغط على Standard test



... Servers found

Hostname	ISP	Country
none	Google	Belgium
none	Google	Belgium
none	Google	Belgium
none	Google	Belgium

...ults of this test mean?

ونلاحظ تغيُر خادم الطلب الى خوادم شركة جوجل



ما هو DNS وما خطورته :

شرح بصورة مبسطة لخدمات DNS وكيف [illegible]

2- تغيير الخادم عن طريق برنامج, وهذه الطريقة أضمن وأقوى.

وهناك العديد من البرامج لتأدية هذه المهمة لكن أفضلها هو OpenDNS فبعد تنصيبه سيعمل دائما مع إقلاع الحاسوب،

ويقوم بتغيير الخادم بشكل تلقائي وربطه مع خادم شركته ويقوم بتشفير البيانات ويمنع التسريب.

ويمكننا تحميل آخر إصدار من البرنامج من موقعه الرسمي:

http://shared.opendns.com/dnscrypt/packages/windows-client/

دعونا نشاهد شرح بسيط لتنزيل البرنامج وتنصيبه وطريقة التعامل معه.



ما هو DNS وما خطورته :

شرح مفهوم نظام أسماء النطاقات DNS وكيف نتفادى خطورته

وهو اختصار لـ Domain Name System هو نظام يخزن معلومات تتعلق بأسماء نطاقات في قاعدة بيانات على الإنترنت.

النطاق / Domain: وهو اسم الموقع الظاهري وله عدة أشكال ولواحق , مثل : Google.com, example.net

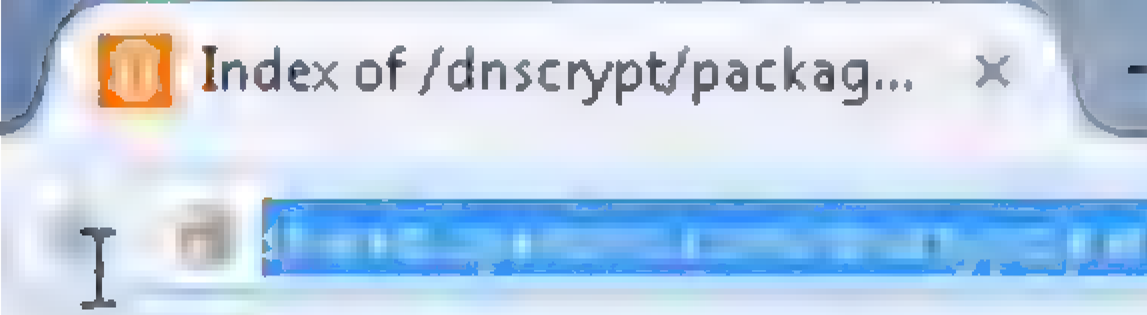
بمعنى آخر DNS هو نظام يقوم بترجمة أسماء النطاقات من كلمات إلى أرقام تعرف باسم IP Address.

فكما أن الهواتف عبارة عن أرقام، فإذا أردت الاتصال بأي هاتف يجب معرفة رقمه، كذلك في عالم الإنترنت

فإذا أردت الاتصال بأي موقع عليك معرفة الـ IP الخاص بهذا الموقع، ولكن بالنسبة للهواتف هناك ما يسمى بخدمة الاستعلامات،

فإذا كنت تعرف اسم أحد الأشخاص، تستعمل هذه الخدمة للحصول على رقمه.

والأمر نفسه بالنسبة لخوادم الإنترنت، فهناك ما يسمى بـ Domain Names/أسماء النطاقات.



Index of /dnscrypt/packages

	Name	Last modified	Size	Desc
	Parent Directory		-	
	DNSCryptWin v0.0.1.zip	21-Mar-2014 06:36	59	





opendns.com

Index of /dnscrypt/packages/windows-client

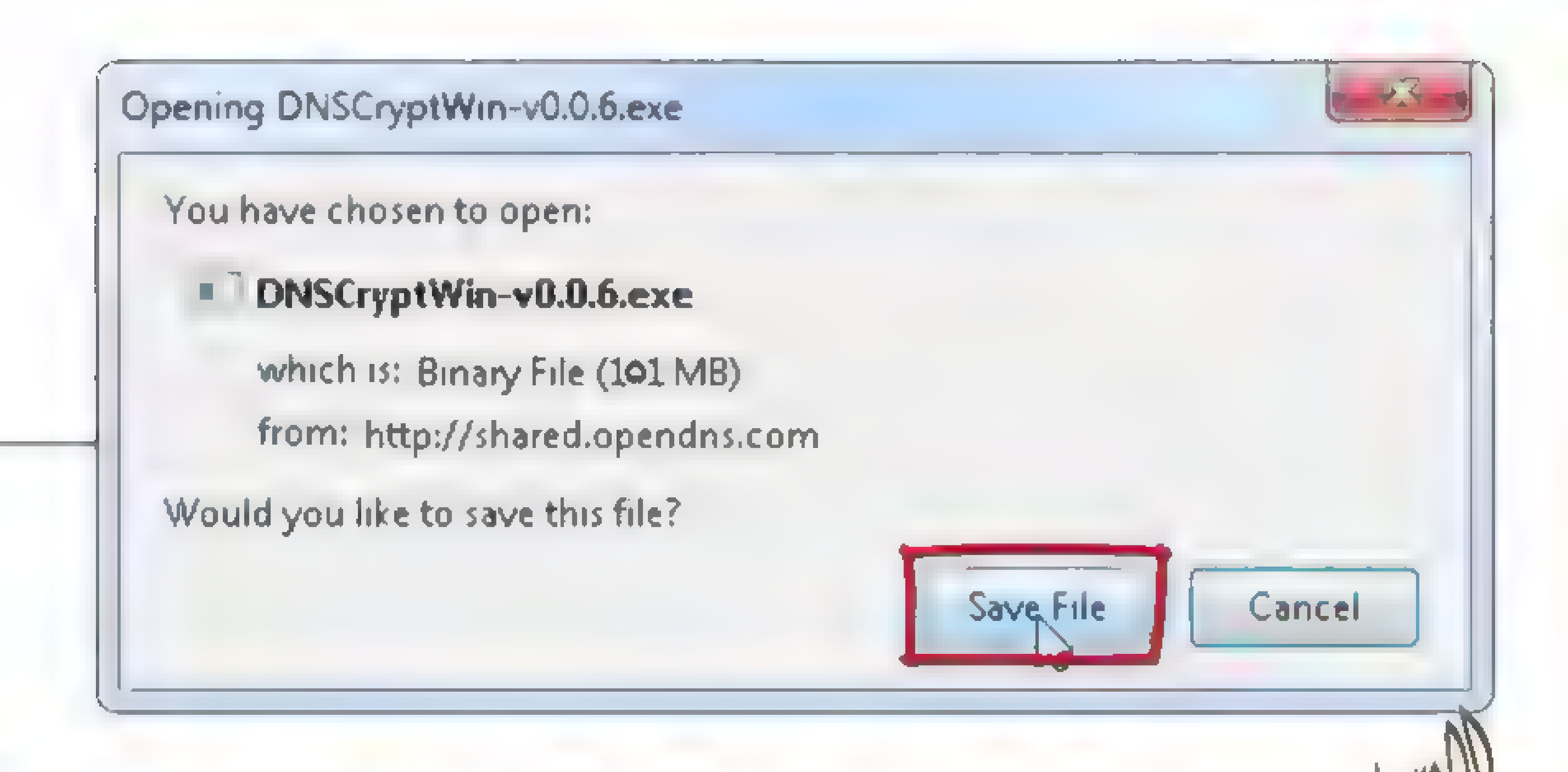
Name	Last modified	Size	Description
 Parent Directory		-	
 DNSCryptWin-v0.0.1.zip	21-Mar-2014 06:36	585K	
 DNSCryptWin-v0.0.3.zip	21-Mar-2014 06:36	595K	
 DNSCryptWin-v0.0.4.exe	21-Mar-2014 06:36	724K	
 DNSCryptWin-v0.0.4.zip	21-Mar-2014 06:36	595K	
 DNSCryptWin-v0.0.5.exe	21-Mar-2014 06:36	720K	
 DNSCryptWin-v0.0.6.exe	21-Mar-2014 06:36	1.1M	

Apache Server at shared.opendns.com Port 80

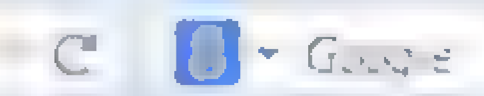


فنية الإسلام

نلاحظ ظهور عدة إصدارات للبرنامج نحمل أحدثها



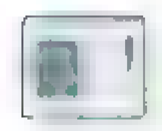
بعد الضغط تظهر لنا نافذة جديدة لحفظ البرنامج المراد تنزيله











DNSCryptWin-v0.0.6.exe

36 seconds remaining — 230 KB of 1.1 MB

Show All Downloads

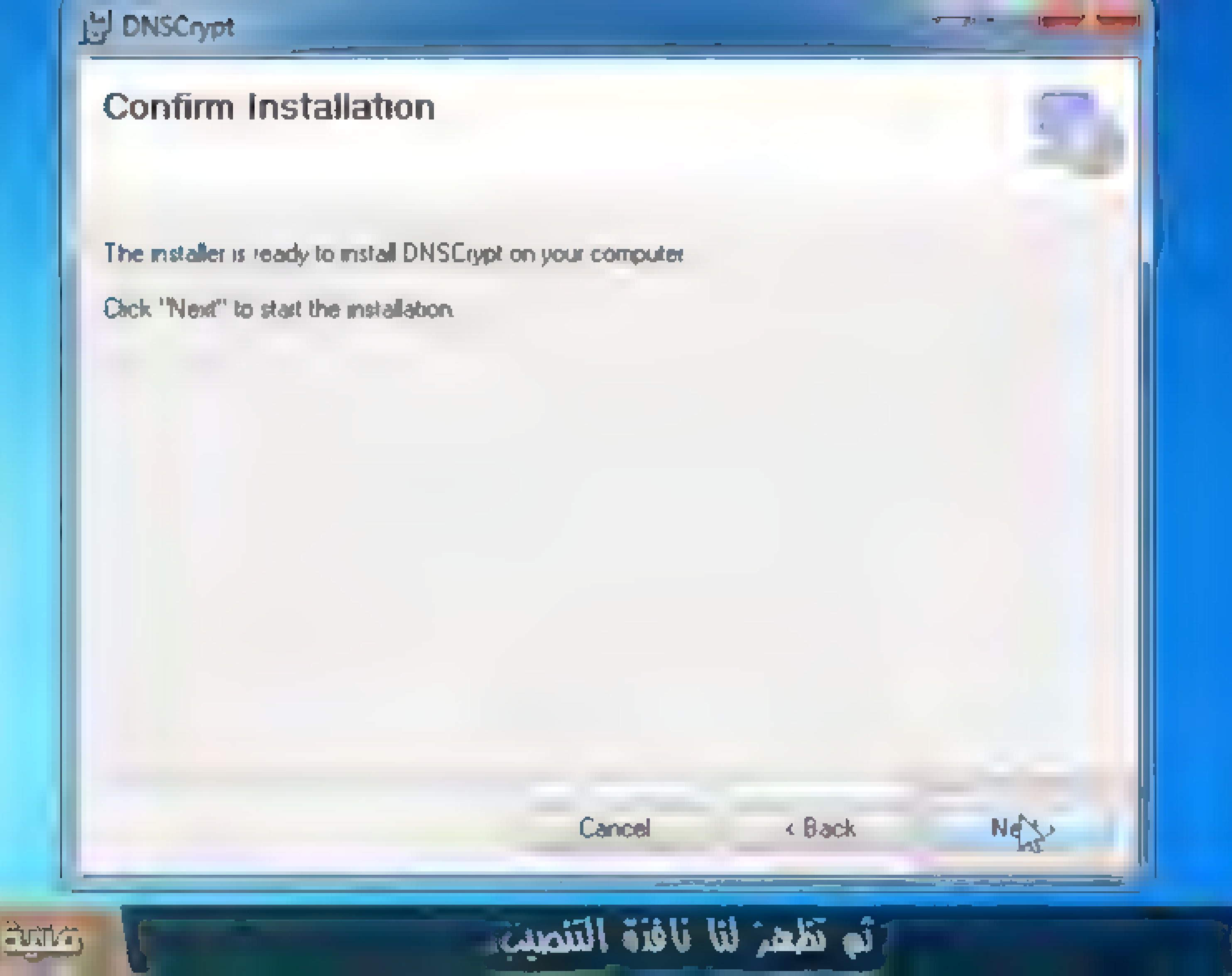


ثم يبدأ المتصفح بتحميل البرنامج





ثم بعد الانتهاء يكون البرنامج بالشكل التالي: نقوم بفتحه



DNSCrypt
Confirm Installation
The installer is ready to install DNSCrypt on your computer.
Click "Next" to start the installation.
Cancel
< Back
Next >
ثم تظهر لنا نافذة التنصيب

Open Control Center

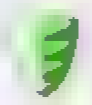
Exit



وبعد الإنتهاء من التنصيب يعمل البرنامج بشكل تلقائي بجانب الساعة

DNS Crypt

General About Release Notes Preview Feedback



Status: Protected

☑ Enable OpenDNS

☑ Enable DNSCrypt

☐ DNSCrypt over TCP / 443 (slower)

☐ Fall back to insecure DNS

Note: Only enable TCP/443 if you use lots of commercial Wi-Fi hotspots at places like Starbucks or GoGo-Inflight Wifi

Current DNS Resolver

208 67 220 220 Using DNSCrypt



http //www opendns com

This software (v 0 0 6) encrypts DNS packets between your computer and OpenDNS This prevents man-in-the-middle attacks and snooping of DNS traffic by ISPs or others

Please help by providing feedback!

If you have a firewall or other middleware mangling your packets, try enabling DNSCrypt with TCP over port 443

If you prefer reliability over security, enable fallback to insecure DNS

صفية الإسلام

نقوم بفتح البرنامج والتأكد من الخيارات الظاهرة

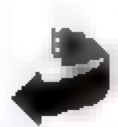


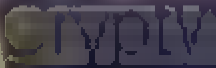


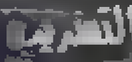
dnsleaktest.com

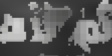
Index of /dnscrypt/package

Name	Last modified	Size	De


Parent Directory








Standard test

Extended test

Whats the difference?



ونضغط على زر Standard test وننتظر انتهاء الفحص



ما هو DNS وما خطورته :

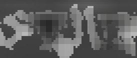
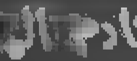
شرح مبسط لخدمة الـ DNS ، وكيف تنتهك خصوصيته

3- الإجابة على الطلب
2- يقوم الخادم بمعالجة الطلب
FaceBook.com
1- إرسال طلب
حاسوبك
DNS Server
root
.net
.com
YouTube

ISP	Country
OpenDNS, LLC	Germany











ما هو DNS وما خطورته :

وبحال استخدمت البرنامج تأكد دائما أن لون أيقونته خضراء بجانب الساعة وإن كانت حمراء فأغلق البرنامج وشغله من جديد.



ما هو DNS وما خطورته :

[illegible] DNS [illegible]

فعندما تريد أن تذهب إلى Google لا داعي أن تكتب IP الخاص بالموقع، فكل ما عليك هو كتابة اسم النطاق.

فيقوم متصفحك بالاستعلام عن الـ IP الخاص بهذا الموقع، ويتم ذلك بإرسال طلب إلى الـ DNS / نظام أسماء النطاقات

ويتم ترجمة الاسم إلى عنوان IP عن طريق نظام أسماء النطاقات

وعندما تريد تصفح الإنترنت بدون حماية كـ «تور» أو «VPN» فعند طلب موقع ما
فإن المتصفح سيرسل طلب للـ DNS الخاص بمزود خدمتك

وخوادم الـ DNS تقوم بتخزين سجلات للطلبات «Logs» فكل طلب يُطلب من هذا الخادم يقوم بتسجيله وتسجيل عنوان طالبه

لكن ما الفائدة من هذا الكلام ؟ وما خطورته ؟



ما هو DNS وما خطورته :

بحالة تصفحنا الإنترنت بحماية أو بدون حماية يجب أن نقوم بخطوة احترازية

ونقوم بتغيير خادم الـ DNS الذي نطلب من خلاله, لمنع أي تسريب في البيانات.

وفي حال طلبنا موقع يتم طلبه من خلال خادم DNS الذي سوف نختاره, ولن يتم الطلب من خادم شركة الاتصال التي نستخدمها.

ويمكن أن يفيد تغيير الـ DNS بزيادة سرعة تصفح الإنترنت ويعود ذلك على حسب سرعة الخادم بالاستجابة للطلبات.

ويمكن استخدام خوادم تقوم بحظر المواقع المخلة بالأدب (أعزكم الله) ويتم ربط «الراوتر» بهذا الخادم ويسري على كل الشبكة.

الآن كيف سنعرف ما هي الخوادم الافتراضية التي نطلب منها ؟ وكيف نغيرها؟



ما هو DNS وما خطورته :

شرح نظام أسماء النطاقات / DNS ، كيف نتفادى خطورته

لتعرف خوادم التي يتم الطلب منها بشكل افتراضي، نذهب للموقع التالي: dnsleaktest.com

طبعاً ندخل للموقع من متصفح عادي بدون حماية لمعرفة النتيجة على الـ IP الحقيقي

بعد الدخول للموقع تظهر لنا معلومات خاصة بنا كعنوان IP وموقعنا الجغرافي، يوجد أسفل المعلومات زرين:

نضغط على الزر Standard Test وبعدها سيقوم الموقع بالفحص.

بعدها سيقوم الموقع بإعطائك نتيجة الفحص ويضع معلومات الخادم كالصورة أسفله مثلاً

Hello 1

from Syria Arab Republic

IP	Hostname	ISP	Country
		Tarassul Inetnet Service Provider	Syria

Standard test | Extended test



ما هو DNS وما خطورته :

شرح مختصر مبسط لتعريف DNS وكيف نتفادى خطره

والآن بعد أن عرفنا المخدمات الافتراضية التابعة لمزود الخدمة, من أين نحصل على مخدمات غيرها؟ وكيف نغيرها؟

يمكننا استخدام مخدمات الشركات الكبرى كـ غوغل أو OpenDNS والكثير غيرها:

Google: 8.8.8.8 And 8.8.4.4 أو OpenDNS: 208.67.222.222 And 208.67.220.220

وإذا كنا لا نريد استخدام هذه المخدمات يمكننا جلب غيرها من الرابط التالي : http://public-dns.tk/

ولتغيير المخدم الافتراضي هناك طريقتين : 1- بشكل يدوي , 2- عن طريق برامج.

ولضمان تغييره واستمراريته وتشفيره والحماية من تسريب البيانات, ننصح باستخدام البرنامج, وسنشرح الطريقتين إن شاء الله.



ما هو DNS وما خطورته :

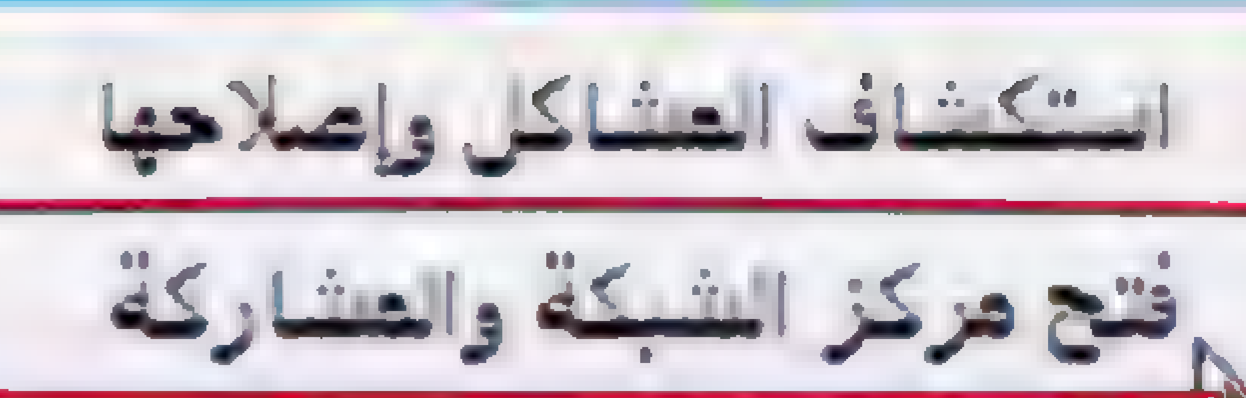
شرح مختصر [illegible] DNS وكيف نتفادى خطورته

1- التغيير اليدوي وهو مفيد بحال أردنا وضع مخدمات مختلفة, أما البرنامج سيلزمنا بخوادم معينة على حسب شركته.

وعند التغيير بشكل يدوي يمكننا وضع مخدم ووضع آخر كبديل, وليس من الضرورة أن يكون هناك بديل.

دعونا نشاهد شرح بسيط لتغيير المخدمات بشكل يدوي, (أنا وضعت مخدم غوغل) لا تتقيد بي ضع ما تشاء

ولا تنسى فحص التسريب بعد وضع المخدم الجديد.



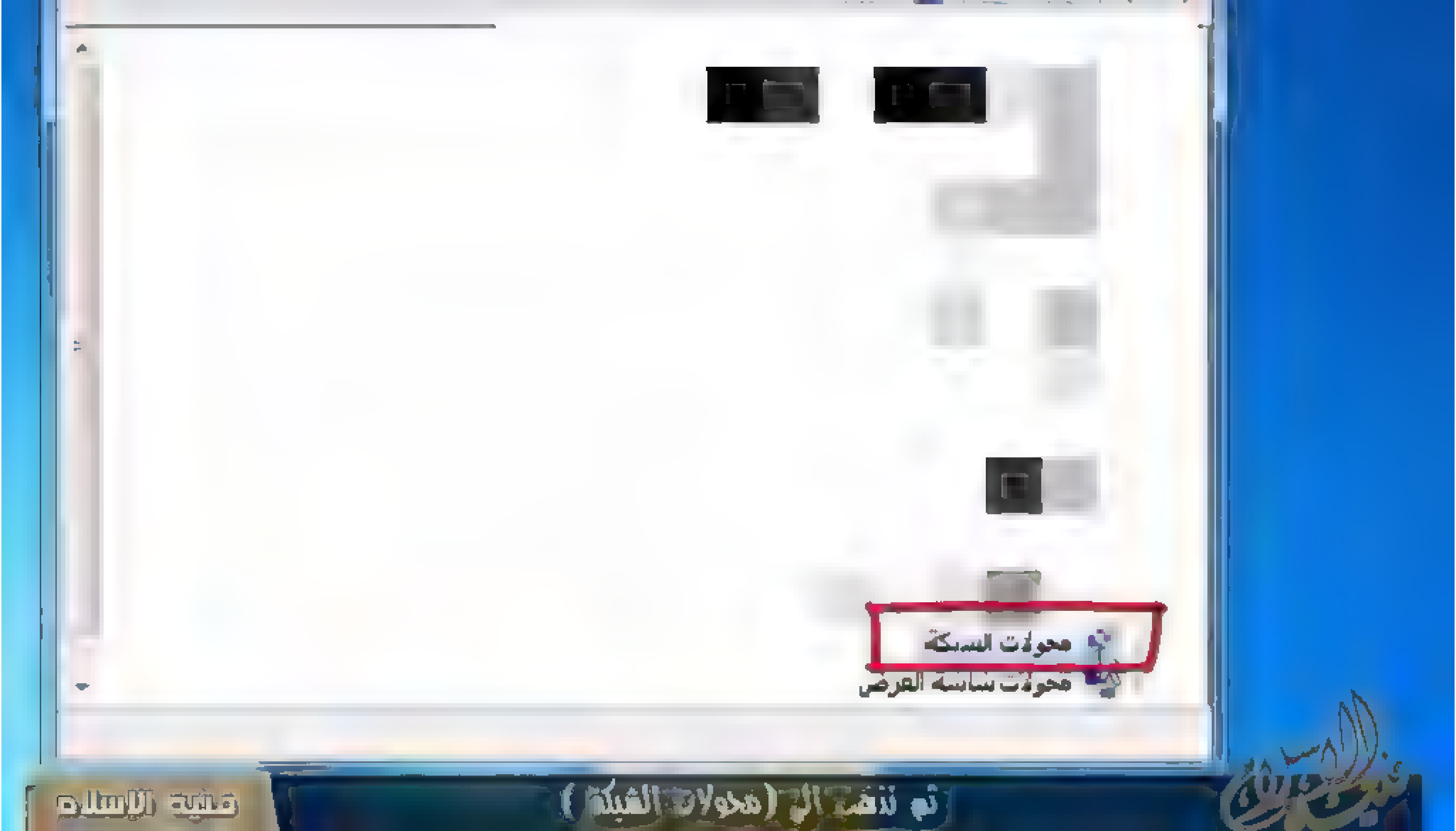
نضغط بالزر الأيمن على رمز الشبكة، ثم نختار (فتح مركز الشبكة والمشاركة)



دورة التخفي والتصفح الآمن للانترنت.

الدرس الخامس.

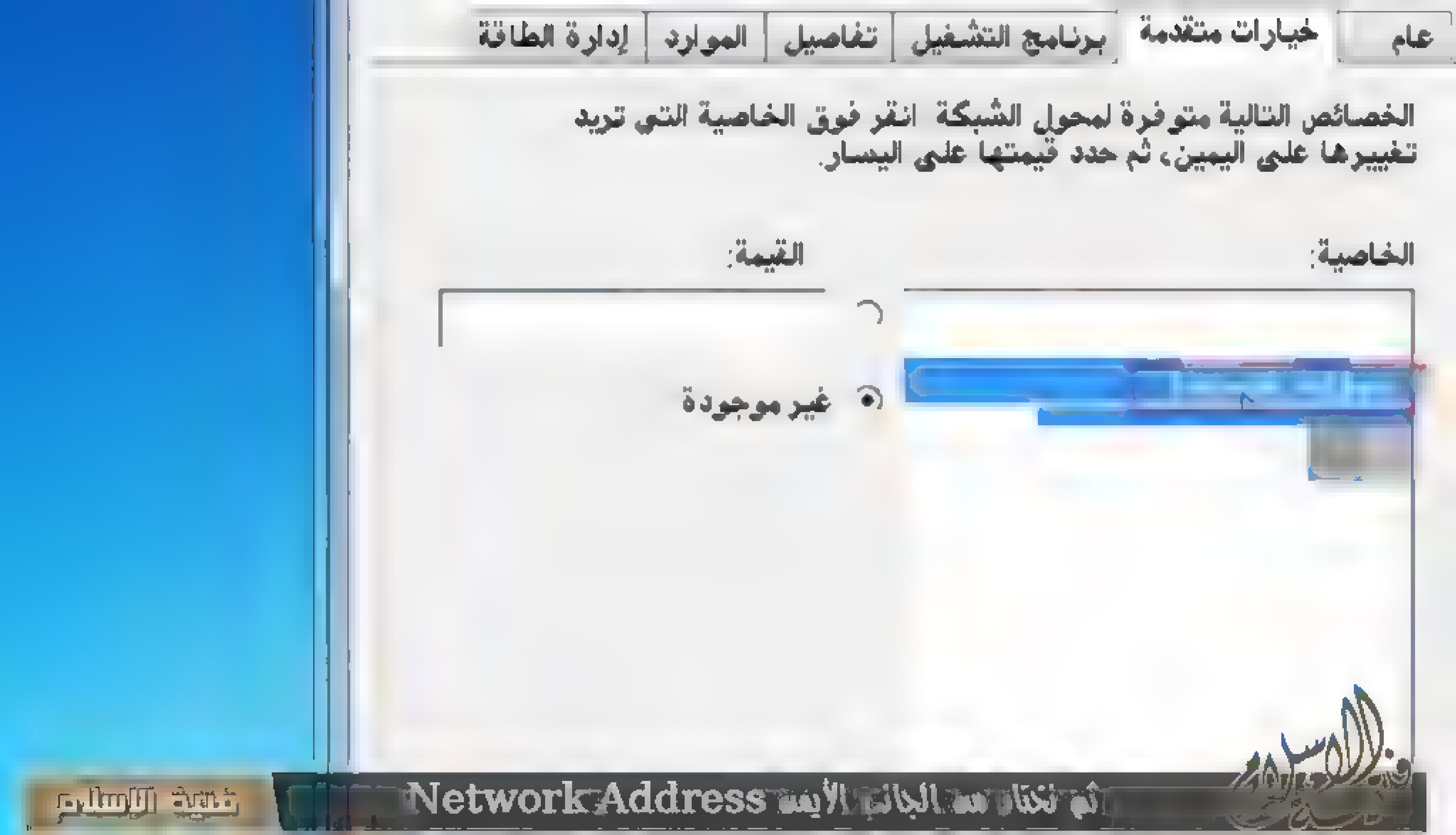
1- ما هو الـMAC أو العنوان الفيزيائي
2- ما خطورته، وكيف أعرفه.
3- تغيير العنوان بشكل يدوي أو عن طريق برامج.


محولات الشبكة
محولات شاشة العرض
ثم نذهب إلى (محولات الشبكة)
تقنية الإسلام

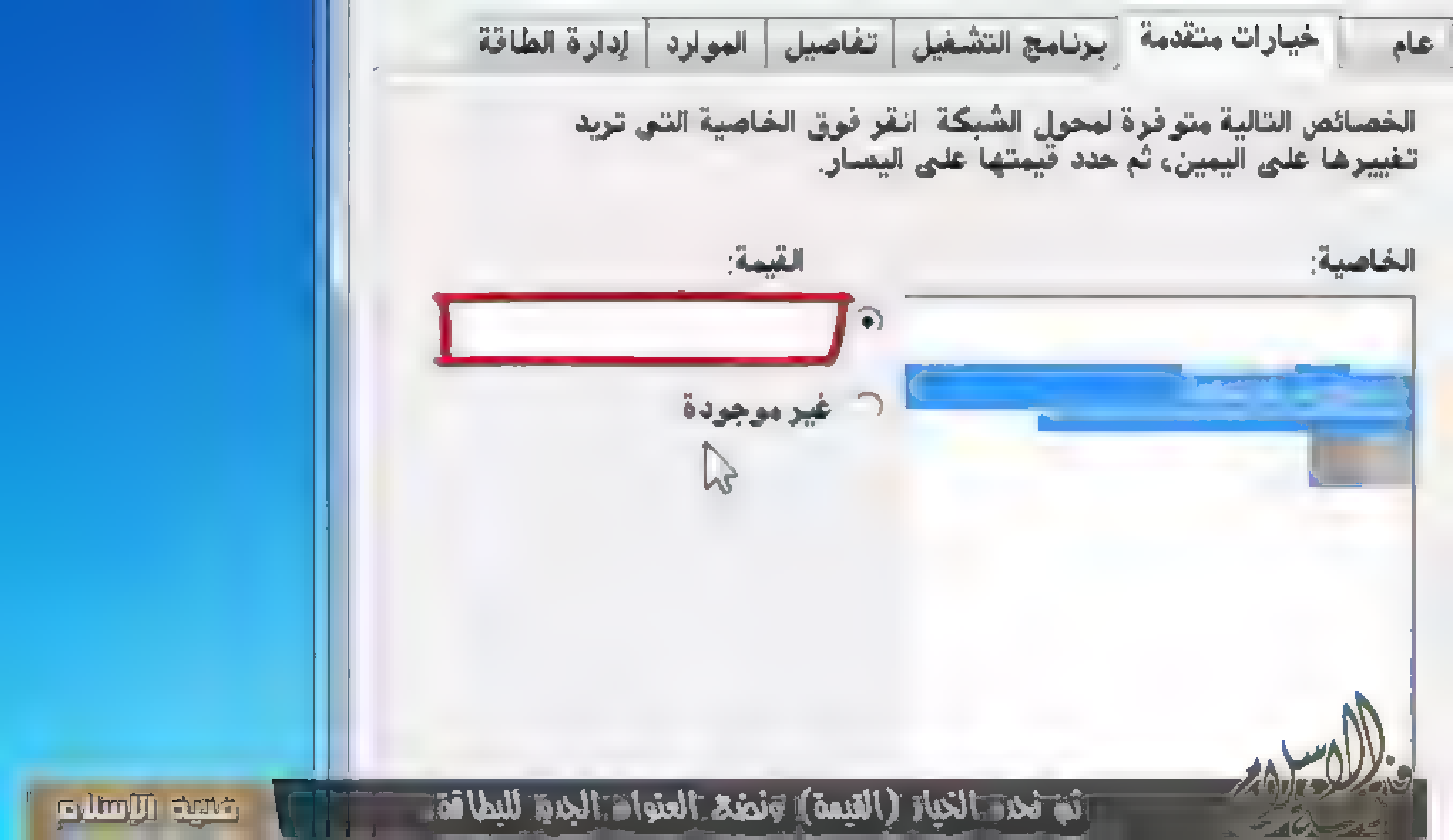

تحديث برنامج التشغيل...
تعطيل
إزالة التثبيت
تفحص تغييرات الأجهزة
الضغط على البطاقة التي تستخدمها بالزر الأيمن ثم خصائص
تقنية الإسلام

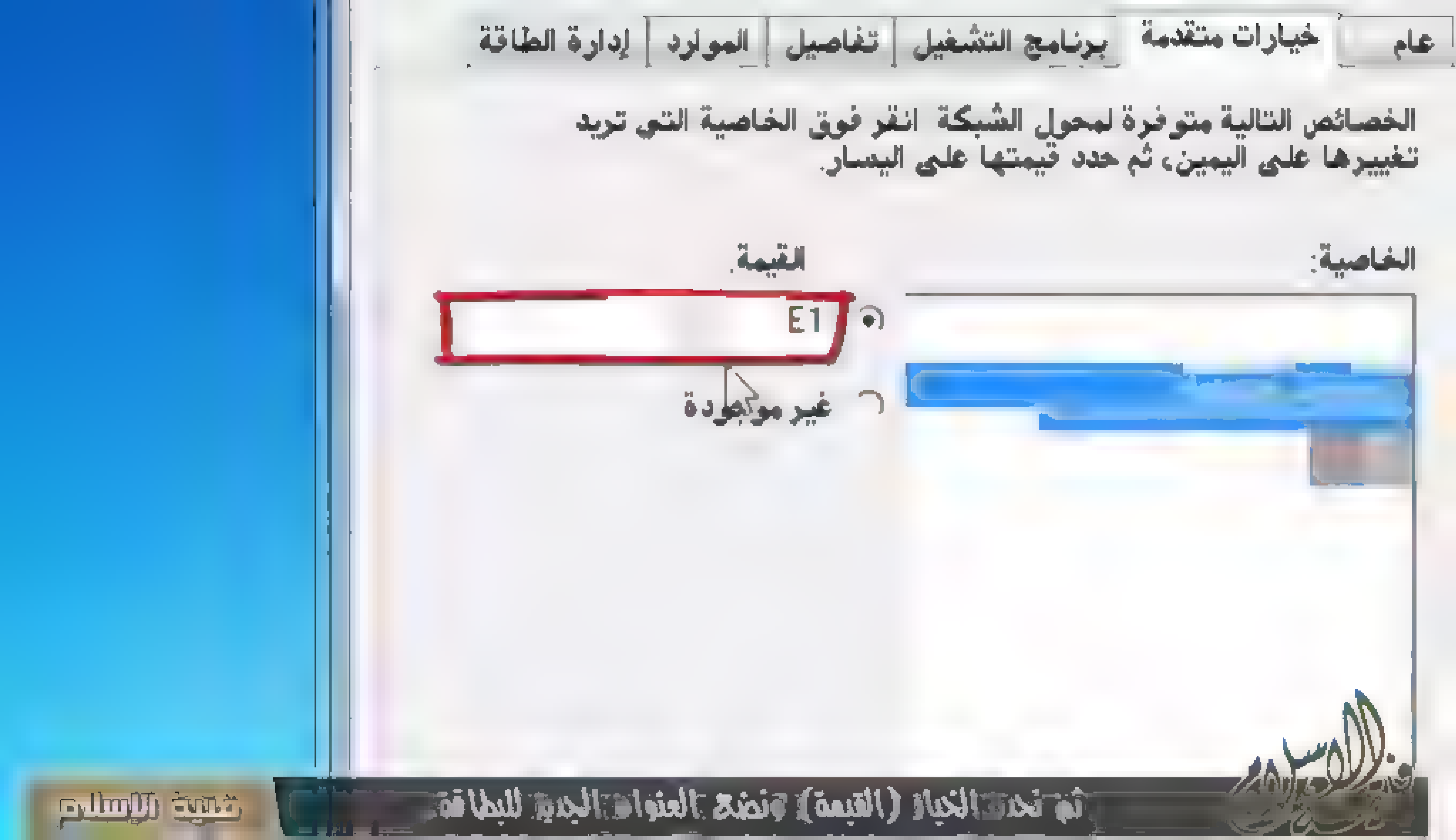


فتظهر لنا نافذة جديدة نضغط على التبويب (خيارات متقدمة)

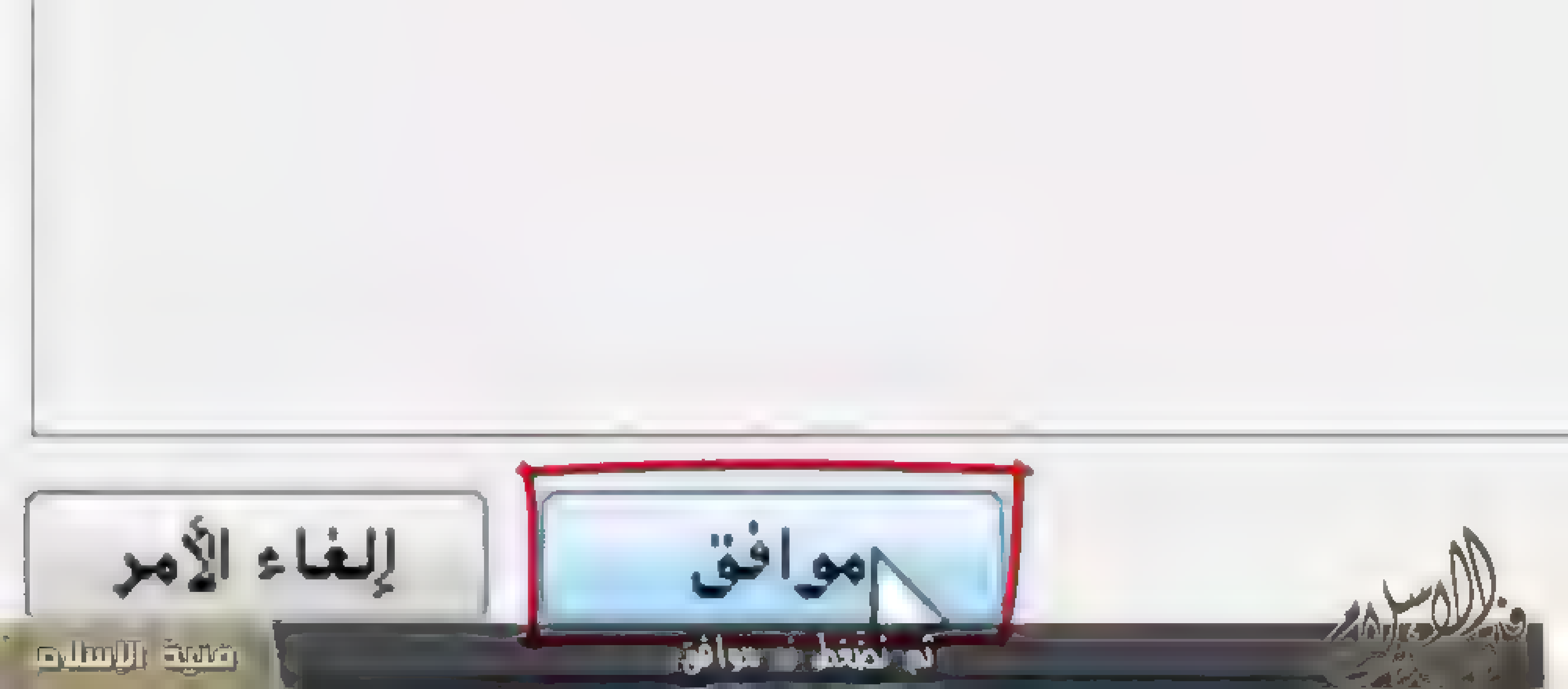


عام
خيارات متقدمة
برنامج التشغيل
تفاصيل
الموارد
إدارة الطاقة
الخصائص التالية متوفرة لمحول الشبكة. انقر فوق الخاصية التي تريد تغييرها على اليمين، ثم حدد قيمتها على اليسار.
الخاصية:
القيمة:
غير موجودة
ثم نختار من الجانب الأيمن Network Address


عام
خيارات متقدمة
برنامج التشغيل
تفاصيل
المولرد
إدارة الطاقة
الخصائص التالية متوفرة لمحول الشبكة انقر فوق الخاصية التي تريد تغييرها على اليمين، ثم حدد قيمتها على اليسار.
الخاصية:
القيمة:
غير موجودة
ثم نحدد الخيار (القيمة) ونضع العنوان الجديد للبطاقة



عام
خيارات متقدمة
برنامج التشغيل
تفاصيل
المورد
إدارة الطاقة
الخصائص التالية متوفرة لمحول الشبكة. انقر فوق الخاصية التي تريد تغييرها على اليمين، ثم حدد قيمتها على اليسار.
الخاصية:
القيمة:
E1
غير موجودة
ثم نحدد الخيار (القيمة) ونضع العنوان الجديد للبطاقة


موافق
إلغاء الأمر
ثم نضغط على موافق



ما هو MAC ADDRESS وما خطورته :

شرح تغيير MAC، [illegible]

2- تغيير العنوان عن طريق برنامج، ويتم ذلك بتنصيب البرنامج «TMAC».

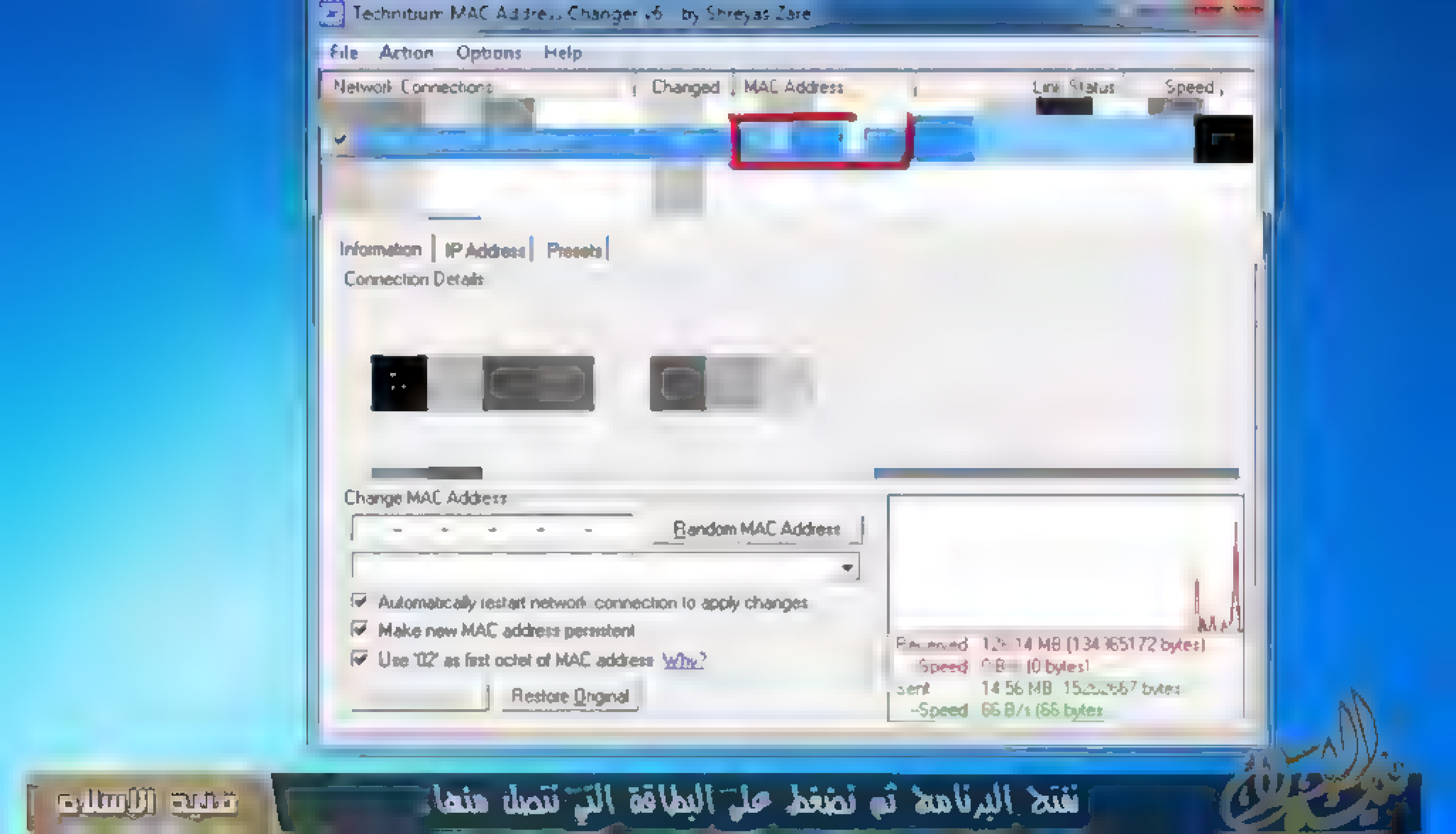
وكل ما علينا تنزيل البرنامج وتنصيبه، وبعدها نفتحه ونضغط على البطاقة المتصلة ونضغط توليد عنوان عشوائي ثم تغيير.

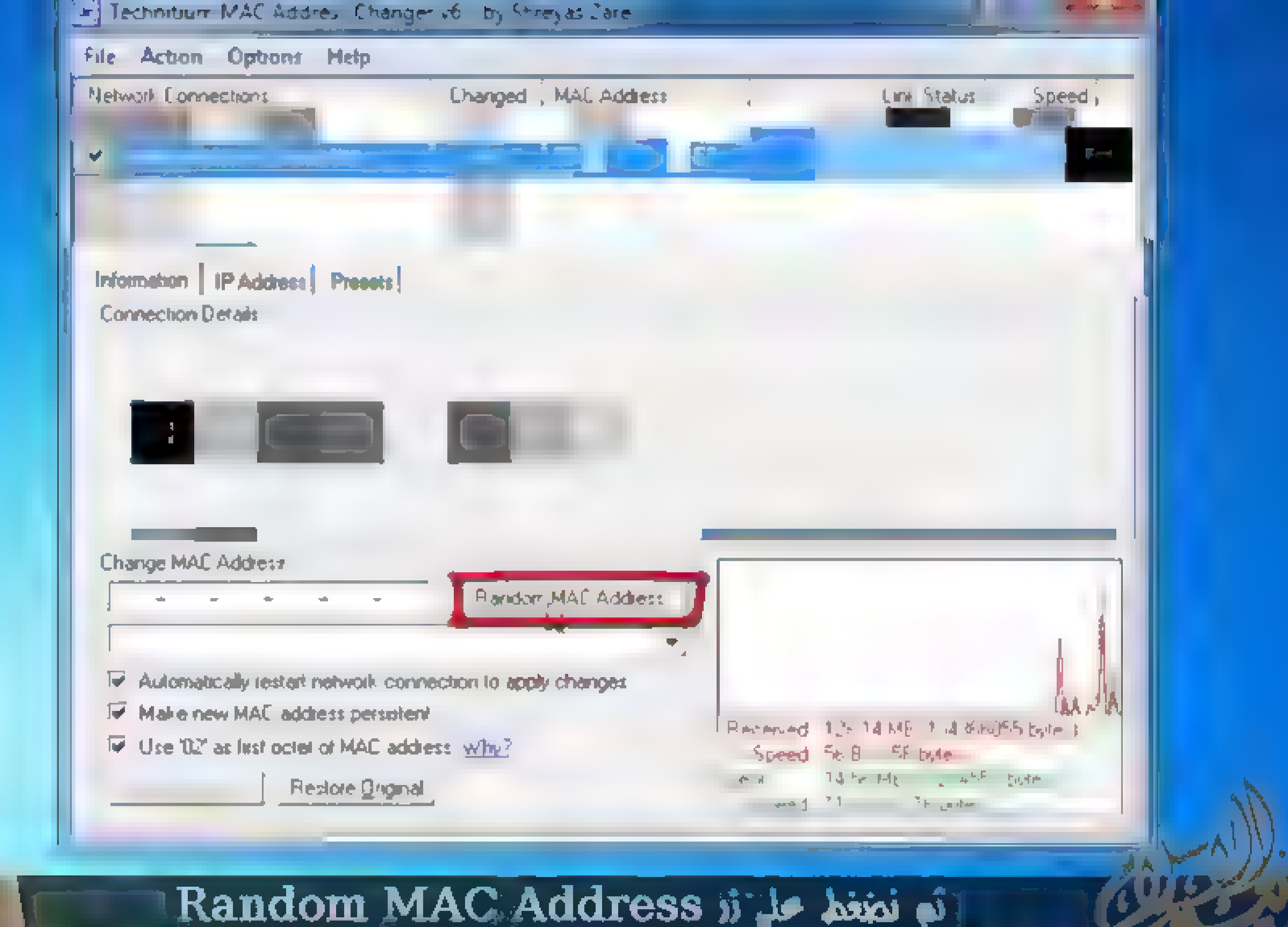
رابط تنزيل البرنامج :

http://download.cnet.com/Technitium-MAC-Address-Changer/3000-2085_4-10554920.html

نفتح الرابط ونضغط على زر «Download Now»

دعونا نشاهد شرح بسيط لطريقة تغيير العنوان عن طريق البرنامج


Technitium MAC Address Changer v6 - by Shreyas Zare
File
Action
Options
Help
Network Connections
Changed
MAC Address
Link Status
Speed
Information
IP Address
Presets
Connection Details
Change MAC Address
Random MAC Address
Automatically restart network connection to apply changes
Make new MAC address persistent
Use '02' as first octet of MAC address Why?
Restore Original
Received
Speed
Sent
Speed
66 B/s (66 bytes
نفتح البرنامج ثم نضغط على البطاقة التي نتصل منها



ثم نضغط على زر Random MAC Address

تنقية الإسلام



ما هو MAC ADDRESS وما خطورته :

شرح العنوان MAC وما الخطر الذي يشكله

العنوان ماك وهو اختصار لـ Media Access Control ويُعتبر قيمة فريدة ترتبط ببطاقة الشبكة من قبل المصنع

والمفروض أن يكون هذا العنوان مميز عالميا أي لا توجد أي بطاقة شبكة أخرى في العالم تأخذ نفس عنوان الماك.

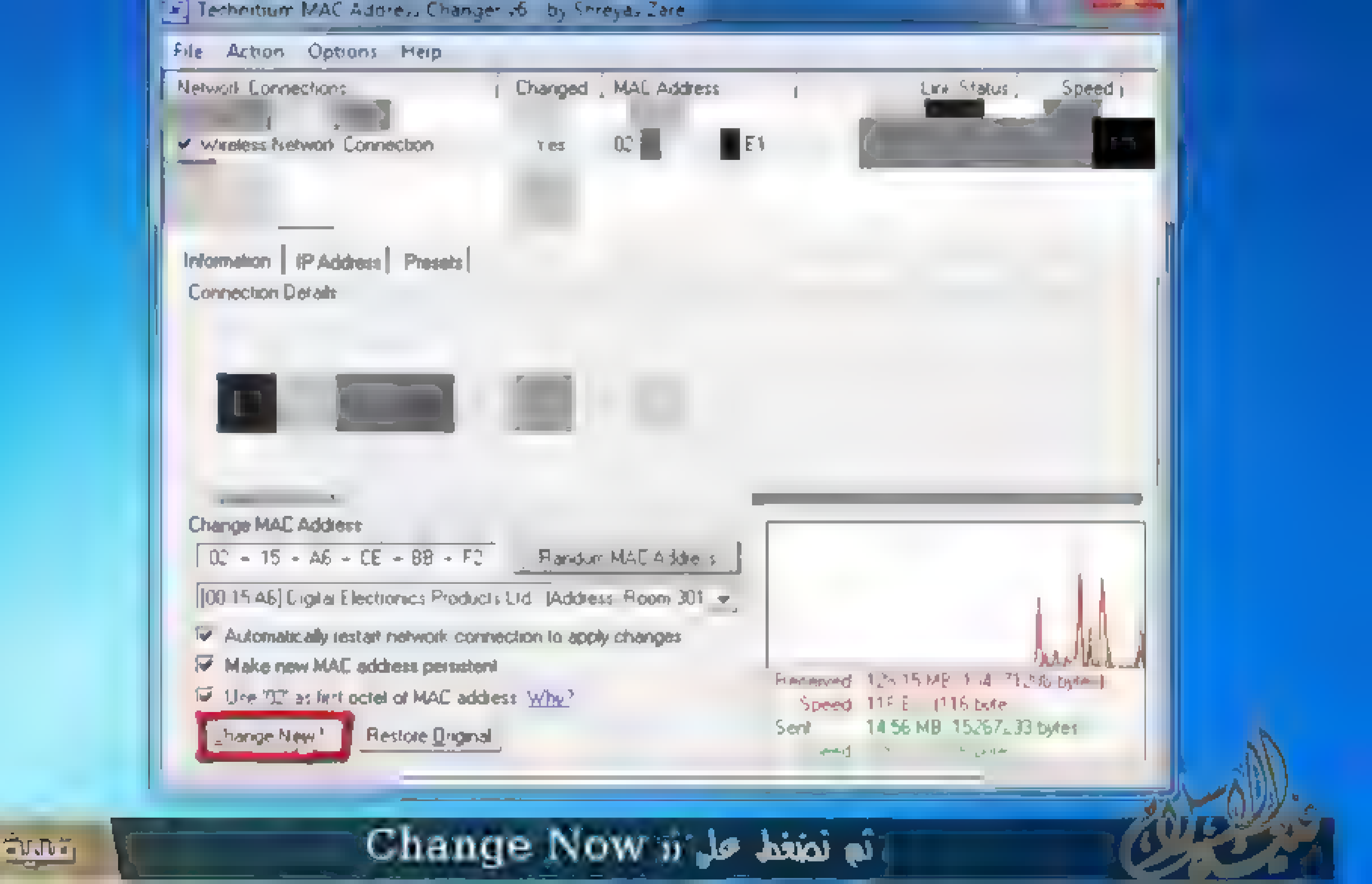
أي كل بطاقة شبكة سلكية أو لا سلكية لها عنوان «MAC» ولا يشبه عنوان أي بطاقة أخرى.

و تتكون هذه العناوين من 12 حرف بالنظام الست عشري, أرقام من 0 الى 9 و حروف من A الى F.

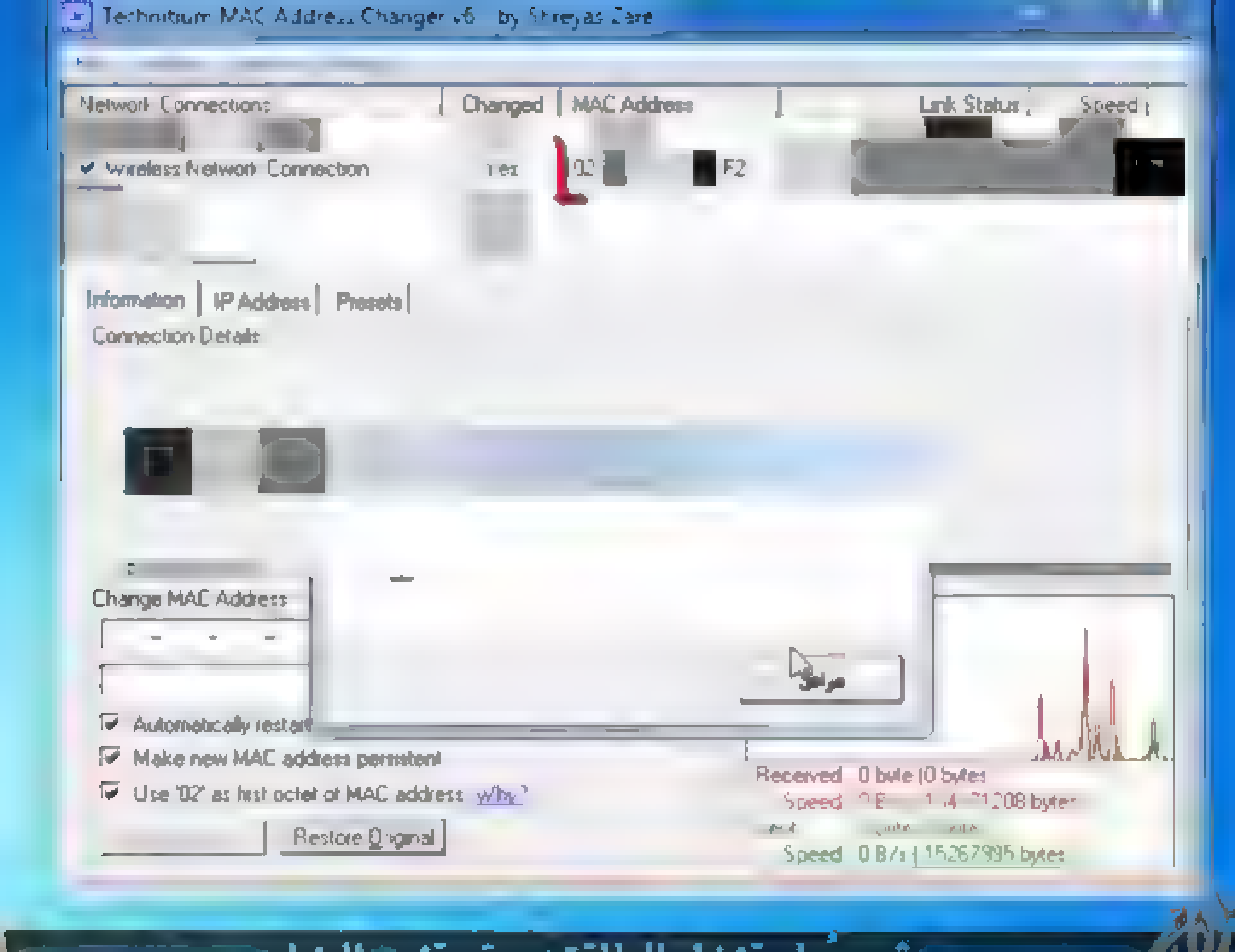
مثال على شكل عنوان «MAC» : 03-A2-65-6F-C3-03

لكن ما الفائدة من هذا الكلام كله ؟

وما الخطورة التي يشكلها هذا العنوان ؟



File
Action
Options
Help
Network Connections
Changed
MAC Address
Speed
Wireless Network Connection
Information
IP Address
Presets
Connection Details
Change MAC Address
Random MAC Address
Automatically restart network connection to apply changes
Make new MAC address persistent
Restore Original
تنمية الإسلام
ثم نضغط على Change Now !!



ثم سيعاد تشغيل البطاقة وسيتم تغيير العنوان



ما هو MAC ADDRESS وما خطورته :

شرح العنوان MAC وما الخطر الذي يشكله

وأنصحكم بأن تغيروا عنوان MAC الخاص بجهازكم كل فترة فلا ضرر في ذلك



ما هو MAC ADDRESS وما خطورته :

شرح لعنوان MAC وما يحصل لي بسببه

بما أن لكل بطاقة شبكة عنوان خاص بها وهذا العنوان مربوط بالشركة المصنعة, فهذا خطر كبير.

فخطورة معرفة عنوان «MAC» الخاص ببطاقتك, لا يقل خطورة عن معرفة IP الخاص بك.

فعند التعرض للتجسس من أي طرف كان, فمعرفتهم لعنوان بطاقتك يشكل خطر كبير, تقريبا كخطر معرفتهم لـ IP الخاص بك.

فكما تحمي الـ IP الخاص بك وتخفيه لكي لا يتم تحديد موقعك, كذلك سنفعل مع عنوان MAC

لكن كيف ساغير عنوان «MAC» الخاص ببطاقتي؟

قبل تغيير عنوان البطاقة علينا معرفة العنوان الحالي, ثم يمكننا تغييره بطريقتين: 1- يدوية | 2- ببرنامج.

كيف أعرف عنوان بطاقتي؟



ما هو MAC ADDRESS وما خطورته :

شرح العنوان MAC ، [illegible]

لتعرف عنوان البطاقة الحالي نذهب لقائمة ابدأ ونكتب CMD ونضغط «انتر»

فتظهر لنا نافذة سوداء نكتب فيها ipconfig /all ثم نضغط «انتر»، فتظهر لنا معلومات البطاقات

ويكون العنوان « MAC» مكتوب بجانب Physical Address أي الرقم الفيزيائي

طبعا يجب الانتباه أنك سوف ترى معلومات البطاقة التي تتصل منها بالإنترنت، لأن المعلومات التي ستظهر تخص كل البطاقات

دعونا نشاهد شرح بسيط لطريقة معرفة عنوان البطاقة الحالي

Administrator: C:\Windows\system32\cmd.exe

```
C:\>ipconfig /all
```

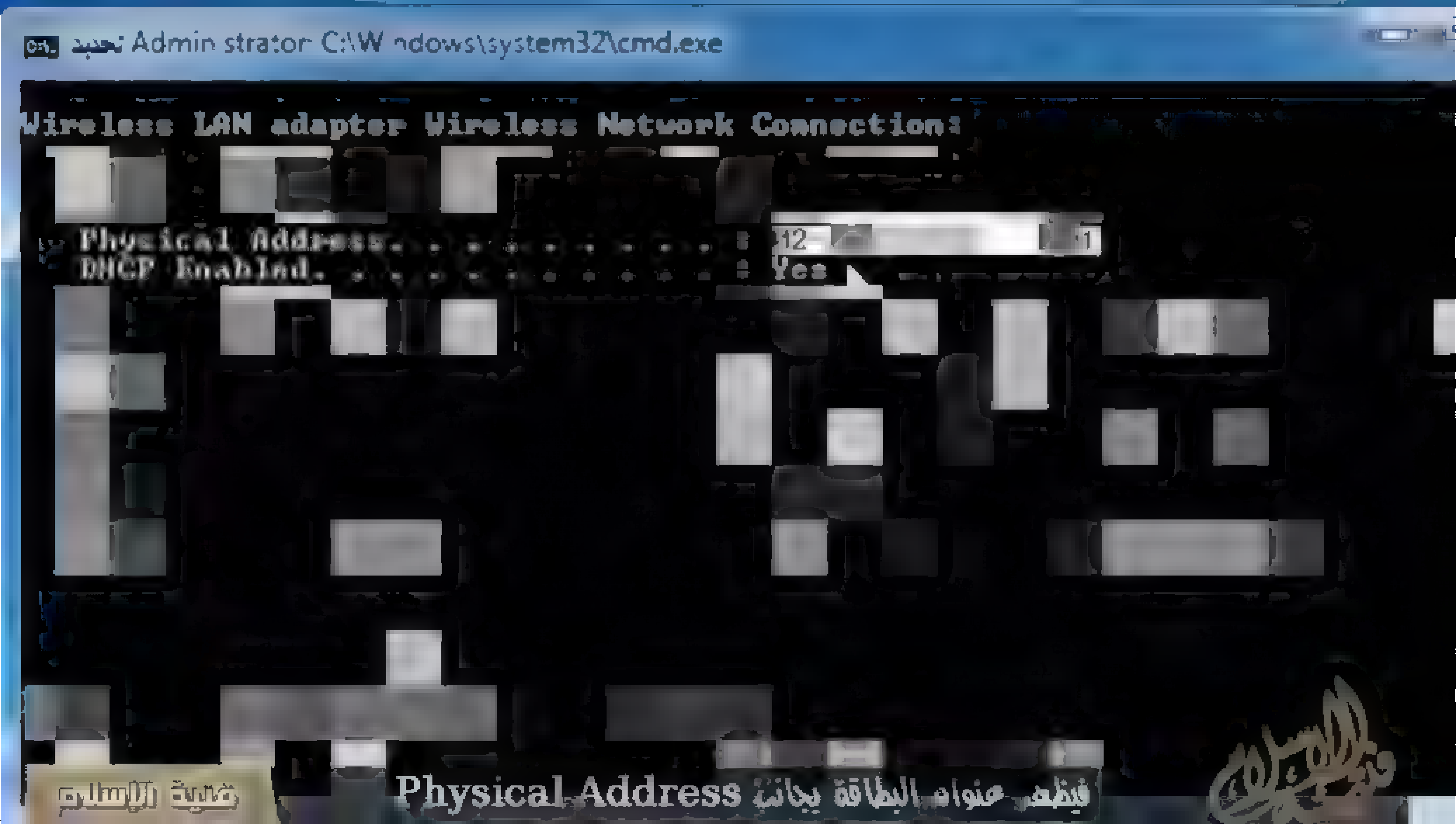
فتفتح لنا نافذة سوداء نكتب فيها ipconfig /all ونضغط (انتر)

Administrator: C:\Windows\system32\cmd.exe

```
Wireless LAN adapter Wireless Network Connection:

   Physical Address. . . . . . . . . : 02-
   DHCP Enabled. . . . . . . . . . . : Yes
```

ثم نذهب للقسم المتعلق بالبطاقة التي نستخدمها للاتصال بالانترنت


تحديد Admin strator C:\W ndows\system32\cmd.exe
Wireless LAN adapter Wireless Network Connection:
Physical Address. . . . . : 12
DHCP Enabled. . . . . : Yes
فتية الإسلام
Physical Address فيظهر عنوان البطاقة بجانب



ما هو MAC ADDRESS وما خطورته :

شرح بسيط عن MAC، ما خطورته على سلامته

1- تغيير العنوان بشكل يدوي، ويتم ذلك بالذهاب لـ «إدارة الأجهزة» ثم «محولات الشبكة»

ثم نختار البطاقة التي نتصل منها بالإنترنت ونضغط عليها بالزر الأيمن ثم نضغط على «خصائص».

فتظهر لنا نافذة جديدة نذهب إلى «خيارات متقدمة» ثم تظهر قائمة فيها عدة خيارات نختار «Network Address»

ونحدد الخيار «القيمة» ثم نضع العنوان الجديد للبطاقة ونضع عنوان عشوائي من 12 خانة مثل التالي 03A2656FC303
ثم نضغط موافق، وبعدها سيتم إعادة تشغيل البطاقة.

دعونا نشاهد شرح بسيط لطريقة تغيير العنوان بشكل يدوي

لوحة التحكم (٢)

إدارة الأجهزة

إدارة الأجهزة الصوتية

لنذهب إلى ابدأ ونكتب (إدارة الأجهزة) ثم نضغط عليها بعد ظهور النتائج



دورة التخفي والتصفح الآمن للإنترنت

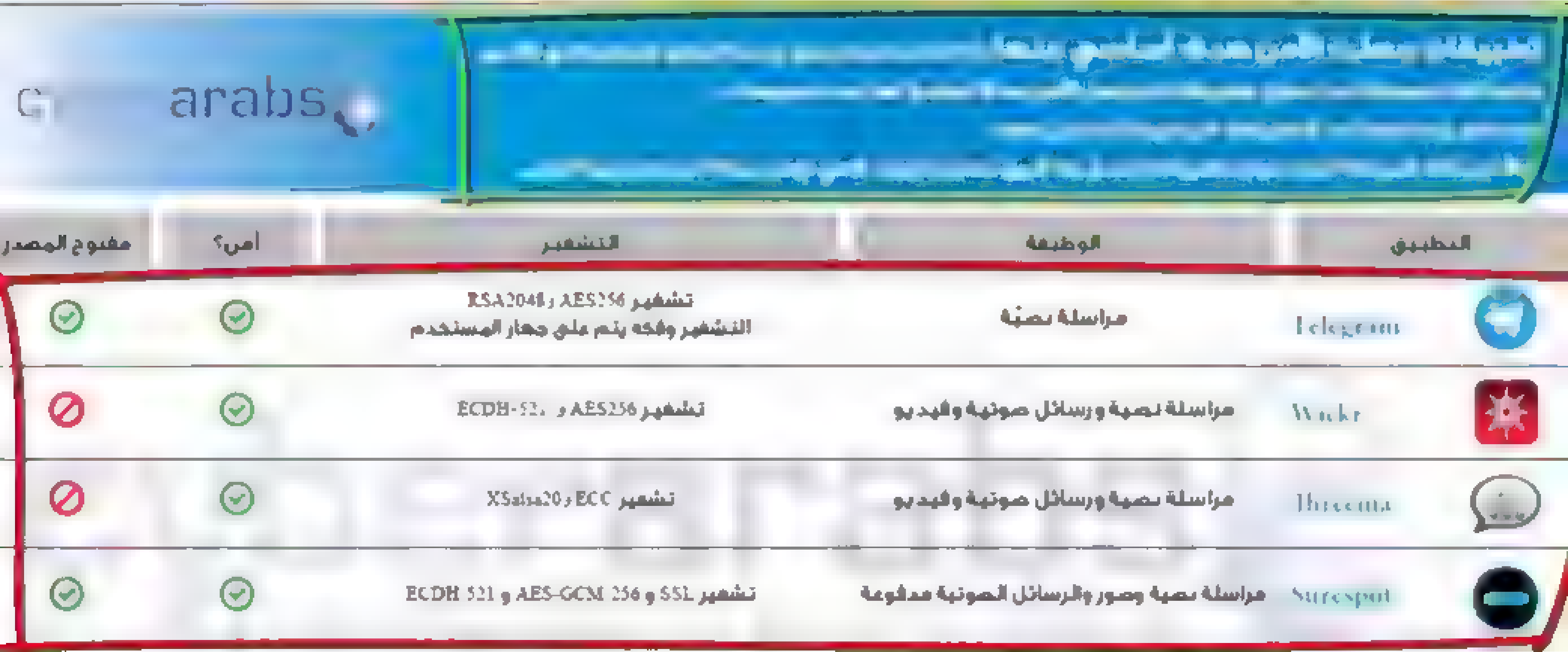
الدرس السادس

1- نصائح عامة يجب الالتزام بها

cyber arabs

تطبيقات وضعت بعض تركيز على الأمن عند تصميمها: قد تكون التطبيقات المذكورة أدناه كافية لحماية اتصالاتكم من بعض المتطفلين أو الأطراف التي لا تتعامل مع شركات هذه التطبيقات

التطبيق	الوظيفة	التشفير	آمن؟	ممنوع المصدر
CoverMe	مراسلة نصية وصوتية	تشفير AES و RSA		🚫
BBM	مراسلة نصية	تشفير SSL ولكن الشركة قادرة على التجسس		🚫
Skype	مراسلة نصية وصوتية وفيديو	تشفير AES256 ولكن الشركة تؤمن للسلطات الحكومية إمكانية التنصت		🚫
iMessage	مراسلة نصية	تشفير End-to-End قابل للتحكم من قبل الشركة		🚫
FaceTime	مراسلة فيديو	تشفير End-to-End قابل للتحكم من قبل الشركة		🚫
Hangouts	مراسلة نصية وصوتية وفيديو	تشفير SSL ولكن الشركة قادرة على التجسس		🚫
Facebook Messenger	مراسلة نصية وصوتية وفيديو	تشفير SSL ولكن الشركة قادرة على التجسس		🚫



التطبيق	الوظيفة	التشفير	آمن؟	مفتوح المصدر
Telegram	مراسلة نصية	تشفير AES256 و RSA2048 التشفير وفكه يتم على جهاز المستخدم	✓	✓
Wickr	مراسلة نصية ورسائل صوتية وفيديو	تشفير AES256 و ECDH-521	✓	⊘
Threema	مراسلة نصية ورسائل صوتية وفيديو	تشفير ECC و XSalsa20	✓	⊘
Surespot	مراسلة نصية وصور والرسائل الصوتية مدفوعة	تشفير SSL و AES-GCM 256 و ECDH 521	✓	✓



SilentCircle	مراسلة صوتية وفيديو (خدمة مدفوعة)	تشفير ZRTP	✓
Redphone	مراسلة صوتية	تشفير ZRTP	✓	✓
Textsecure	مراسلة نصية	تشفير مشتق من OTR	✓	✓
OSTel	مراسلة صوتية	تشفير ZRTP و SRTP	✓	✓
ChatSecure	مراسلة نصية	تشفير OTR	✓	✓

آمن/مفتوح المصدر — غير آمن/مغلق المصدر — آمن إلى حدّ ما/جزء من المصدر مفتوح

نصائح عامة :

ولمعرفة معلومات أكثر وكل ما هو جديد بخصوص برامج التراسل وحمايتها،
تجد ذلك على موقع منظمة EFF العالمية، على الرابط التالي:
https://www.eff.org/secure-messaging-scorecard



نصائح عامة :

لضمان حماية على حسابك [illegible]

- اختيار كلمة مرور معقدة لحسابك واجعلها خليطاً من الحروف والرموز والأرقام.
- لا تضع كلمة مرور موحدة لكل حساباتك.
- لا تثق بأي شخص كان، ولا تتكلم بمعلومات تخصك مع أي شخص كان، لأن اختراق العقول أهم بكثير من اختراق الحواسيب، لذلك انتبه لكل ما تقوله وتكتبه.
- لا تضع أي معلومة شخصية عنك بأي موقع، وبعض المواقع تطلب توثيق عبر الهاتف، فابحث عن موقع تعطيك رقم مجاني.
- دائما حاول قدر الإمكان أن تتصفح المواقع التي تدعم التشفير كـ SSL.
- لا تفتح أي رابط مشبوه، وهذا موقع لفحص الروابط safeweb.norton.com.
- لا تخزن أي كلمة مرور من كلماتك في المتصفح.

نصائح عامة :

[illegible]

- عدم استقبال أي ملفات من أحد وعدم فتحها وخصوصا الملفات ذات الصيغ التنفيذية التي تكون لاحقتها exe أو Src وهناك الكثير من الصيغ التنفيذية
- عندما تنتهي من تصفح حسابك يفضل أن تسجل الخروج منها.
- عند التعامل مع الفيس بوك, تأكد من تفعيل إعدادات الحماية كسؤال الأمن والأصدقاء الموثوقين والرموز السرية.
- تأكد من إخفاء معلوماتك السرية كتاريخ الميلاد والبريد, وننصح دائما بعدم وضع معلوماتك الحقيقية, وعدم وضع رقم الهاتف.
- تأكد دائما أن حساباتك في تويتر وفيس بوك خالية من التطبيقات, ويتم معرفة التطبيقات من خلال اعدادات الحساب.
- وننصح عدم استخدام برامج وسيطة للتغريد أو النشر على فيس بوك.
- وننصح دائما بمسح رسائل الحسابات بشكل دوري.

فتية الإسلام

نصائح عامة :

- ننصح بعدم وضع صور لكم أو لأماكن تواجدكم على الإنترنت، وحتى لو كانت لا تظهر شيء شخصي، لأن هناك معلومات خطيرة تكون مع الصورة، وتشمل هذه المعلومات مكان التقاط الصورة والكاميرا التي تم التصوير بها والكثير من المعلومات الخطيرة وتسمى هذه المعلومات بـ Metadata.

- ولا ننصح بالتواصل عبر تطبيقات المراسلة على الهواتف وخصوصا بالمعلومات المهمة والحساسة، لأنه يمكن إعادة استخراج كل معلوماتك ورسائلك ولو حذفتها من هاتفك وقمت بعمل فورمات له حتى، وهذا الأشياء شبه بسيطة بالنسبة لمحققين الجنائيين.

- وننصح دائما بإلغاء تفعيل أنظمة الملاحة GPS من الهاتف، وبشكل عام لا ننصح باستخدام الهواتف لأنها لا تؤمن حماية.

- التأكد من حماية جهاز الإنترنت "الراوتر" بوضع كلمة مرور قوية للشبكة اللاسلكية ولوحة التحكم لضمان منع اختراق الراوتر من قبل هاكر والتجسس عليه.

نصائح عامة :

[illegible]

- ونتأكد أيضاً من إلغاء نظام **WPS** من الراوتر بحل وجودهم وأيضاً نقوم بإلغاء بروتوكول **UPnP** لأنهما يشكلان خطر ويسهلان اختراق الراوتر، وطبعاً كل ما عليك هو الدخول للوحة الراوتر ووضع معلومات الدخول، وغالباً تجد المعلومات أسفل الراوتر أو مرفقة معه والبحث عن الخدمات التي ذكرناها وإيقافها ويمكنك الاستعانة بالكتيب المرفق مع الراوتر، وهذه الخطوات للأمن مهم لاختراق الراوتر من قبل الهكر والتجسس علينا.

- هناك عديد من المصادر أكدت أن الشركات الكبرى كـ جوجل ومايكروسوفت وفايرفوكس تستطيع تحديد موقعك عند استخدامك أحدى منتجاتها يتم تحديد موقعك عن طريق جهاز الإنترنت (الراوتر) وتخزن عنوان **SSID** الخاص بالراوتر ومعلومات أخرى ولذلك ينصح بوضع كلمة **_nomap** بعد اسم الشبكة الخاصة بك، وذلك يخبر روبوتات الشركة أنها لا تأخذ معلومات الواي فاي الخاص بك، كل ما عليك هو الدخول للوحة الراوتر ثم إعدادات الوايرلس ثم تجد معلومات الشبكة وكل ما عليك إضافة الكلمة بعد اسم شبكتك مثال : **My Nerwork_nomap**

فتية الإسلام

نصائح عامة :

- ننصح دائما بعدم استخدام تطبيقات المراسلة المشهورة كالواتس آب والفايبر والسكايب والتانغو وغيرهم، فإنها تطبيقات غير آمنة وقد تشكل خطراً عليكم ولا تراعي أي خصوصية وأغلبها يستطيع الوصول الى محتويات هواتفكم ويقومون بالمتاجرة بمعلوماتكم الشخصية ويبيعونها للمخابرات وشركات أخرى مهما كانت المعلومات بسيطة.

وبحالة استخدام برامج المراسلة المباشرة ننصح باستخدام « Telegram » فهو يقوم بتشفير قوي وله خواص قوية كـ نظام المحادثات السرية وخاصية التدمير الذاتي للرسائل، وأيضا يمكن استخدام « Threema» وهذان البرنامجان نُصح بهما من قبل الكثير من خبراء الأمن المعلوماتي.

- لا تثق ببرامج المراسلة كاسم البرنامج أو اسم الشركة المنتجة، بل اهتم بطريقة عمل البرنامج وما الخصوصية التي يؤمنها، لأن برامج الشركات الكبرى كلها غير آمنة وتتاجر بعملائها وتتجسس عليهم وتبيع بياناتهم لمخابرات بلادهم أو لشركات اجتماعية.

نصائح عامة :


وإليكم هذا التقرير الذي قام به أحد المواقع الأمنية العربية ويتحدث عن برامج المحادثة المباشرة



تطبيقات لم يجعل الأمن هدف أساسي عند تصميمها

التطبيق	الوظيفة	التشفير	آمن؟	مفتوح المصدر
Viber	مراسلة نصية وصوتية	غير مشفر يقوم بتمويه الصوت فقط	⊘	⊘
WhatsApp	مراسلة نصية ورسائل صوتية	تشفير ضعيف جداً أشبه بعدم التشفير	⊘	⊘
LINE	مراسلة نصية وصوتية وفيديو	تشفير SSL فقط عند استخدام WIFI يتم تعطيله عن استخدام 3G 4G	⊘	⊘
Tango	مراسلة نصية وصوتية وفيديو والعاب	لم يتم التصريح عن أي تشفير	⊘	⊘
ooVoo	مراسلة فيديو	لا يقوم بأي تشفير	⊘	⊘
Kakao Talk	مراسلة نصية وصوتية	تشفير SSL فقط عند استخدام WIFI يتم تعطيله عن استخدام 3G 4G	⊘	⊘
WeChat	مراسلة نصية وصوتية وفيديو	تشفير SSL للاتصال وضع SQLC للبيانات ولكن يوجد به ثغرات أمنية	⊘	⊘
Nimbuzz	مراسلة نصية وصوتية	لم يتم التصريح عن أي تشفير	⊘	⊘



Nimbuzz	مراسلة نصية وصوتية	لم يتم التصريح عن أي تشفير	⊘	⊘
Hike	مراسلة نصية ورسائل صوتية	تشفير SSL فقط عند استخدام WIFI يتم تعطيله عن استخدام 3G 4G	⊘	⊘
Chat ON	مراسلة نصية ورسائل صوتية	تشفير SSL لكن الملفات التي تتم مشاركتها لا يتم تشفيرها	⊘	⊘
Kik	مراسلة نصية	غير معروف	⊘	⊘
Voxer	مراسلة صوتية	غير معروف	⊘	⊘
GroupMe	مراسلة نصية	غير معروف	⊘	⊘
MessageMe	مراسلة نصية	غير معروف	⊘	⊘
Imo.im	مراسلة نصية وصوتية	غير معروف	⊘	⊘
TalkRay	مراسلة نصية ورسائل صوتية وفيديو	غير معروف	⊘	⊘
IM+	مراسلة نصية	لا يقوم بالتشفير ولكن يدعم تشفير OTR	⊘	⊘



دورة التخفي والتصفح الآمن للإنترنت

الدرس السابع (الخطوات المتقدمة)

1- ما هي توزيعة Tails

2- ما هو الـ RDP وكيف تحصل عليه

3- التشفير المتقدم للرسائل و الملفات

الخطوات المتقدمة:

الأساليب التي ذكرناها سابقا هي طرق بسيطة لحماية خصوصيتنا ولتصعيب المهمة إلى أكبر قدر ممكن لكن من يريد القيام بأمور جدية ويحتاج إلى مزيد من الخصوصية عليه بهذه الخطوات المتقدمة

وهذه الطرق تساعدك لكي تكون مجهول الأثر وتخفي أثرك بشكل أكبر فهي من الخطوات المتقدمة

- توزيعة Tails
- ما هو الـ RDP وكيف نحصل عليه
- التشفير اليدوي للرسائل والملفات



توزيعة TAILS:

وهي توزيعة مبنية على نظام لينوكس ولمن لا يعرف لينوكس هو نظام تشغيل يوجد له الكثير من الإصدارات

ونسبة قليلة في الوطن العربي تستخدمه فالأغلب يستخدم إصدارات ويندوز من مايكروسوفت

ويعتبر نظام لينوكس بشكل عام أكثر حصانة وأمنا من الويندوز

وبالنسبة لطريقة استعمال هذه التوزيعة يمكنك أن تضعها على مفتاح USB أو على CD وتشغل التوزيعة عند إقلاع الجهاز

وتتصفح الإنترنت بخصوصية أكثر وتحوي التوزيعة على نسخة تور للتصفح من خلالها

وأهم ما في هذه الطريقة أن تستخدم الإنترنت من دون تخزين أي شيء فعندما تفصل التوزيعة من الUSB Flash تكون تصفحت

بالتالي لن يكون هناك أي معلومات مخزنة ولن يكون هناك أي أثر لك

فتية الإسلام

توزيعة TAILS:

ومما يميز التوزيعة أنها متوفرة بشكل ويندوز XP لكي لا يشك بك أحد

ولصعوبة شرح التوزيعة بشكل مفصل, اخترت لكم فيديو من الانترنت يسهل عليكم فهم هذه التوزيعة:

http://www.youtube.com/watch?v=N7bA7xm-o

وهذا رابط لتحميل التوزيعة من موقعها:

https://tails.boum.org/download/

واعلم أن الشركة التي صنعت هذه التوزيعة هي نفسها شركة برنامج تور.



ما هو RDP وكيف أحصل عليه:

وهو بروتوكول للاتصال في Remote Desktop Protocol ويستخدم للاتصال بسطح مكتب بعيد

أي حاسوب بعيد موجود على خادم ما تركب عليه أنظمة التشغيل ويتمتع بخط قوي وسرعة انترنت عالية ويصل دورنا أن نقوم

نستطيع تسجيل الدخول إليه وكأنه حاسوبنا الشخصي، والتحكم به كما نريد وكأنه حاسوب أمامنا،

وهذا يضمن لنا سرية وخصوصية أعلى بالقيام بأعمالنا على الإنترنت

لكن ما يعيق البعض لاستخدام هذه الخدمة هي أنها مدفوعة في معظم الأحيان

وبحال وجود مواقع تقدم هذه الخدمة بشكل مجاني فستكون الخدمة لمدة محدودة

لكن لا بأس يمكنك بعد الانتهاء من المدة التجريبية بإعادة التسجيل بالموقع مجددا واستعمال الخدمة من جديد

ما هو RDP وكيف أحصل عليه:

وستظهر لكم مواقع تتيح هذه الخدمة مجانا ويمكنكم بعد انتهاء الفترة التجريبية عمل حساب جديد والدخول للخدمة من جديد

كل ما عليكم هو الدخول لأحد هذه المواقع والتسجيل كما في أي موقع

ثم سيصل لكم ملف صغير وهو الملف الذي ستفتحونه للاتصال بالحاسوب البعيد

عن طريق اسم مستخدم وكلمة مرور اللذان سيأتيان [illegible] وبعد الاتصال ستظهر نافذة الحاسوب البعيد

ولكن قبل الاتصال يجب عليك التأكد من جهازك يسمح بالاتصال بسطح مكتب بعيد.

اذهب لابدأ واكتب خصائص فتظهر لنا النتائج نضغط على خصائص ثم نضغط على الإعدادات عن بعد من يمين النافذة

فتظهر لنا نافذة جديدة نضع الإشارة على مربع السماح باتصالات المساعدة عن بعد لهذا الكمبيوتر ثم نضغط موافق

ما هو RDP وكيف أحصل عليه:




نذهب الى ابدا ونكتب (النظام) وننتظر ظهور النافذة ونضغط عليه

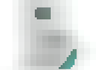

برامج (٥)
معلومات النظام
تكوين النظام
استعادة النظام

البرامج (٥)

- معلومات النظام
- تكوين النظام




- استعادة النظام

- إنشاء قرص "إصلاح النظام"



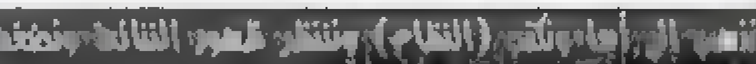

- مراقبة النظام



لوحة التحكم (٤٢)



- النظام



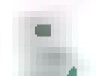
البرامج (٥)

معلومات النظام

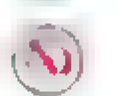
تكوين النظام



استعادة النظام



إنشاء قرص "إصلاح النظام"



مراقبة النظام

لوحة التحكم (٤٣)

النظام



الصفحة الرئيسية للوحة التحكم

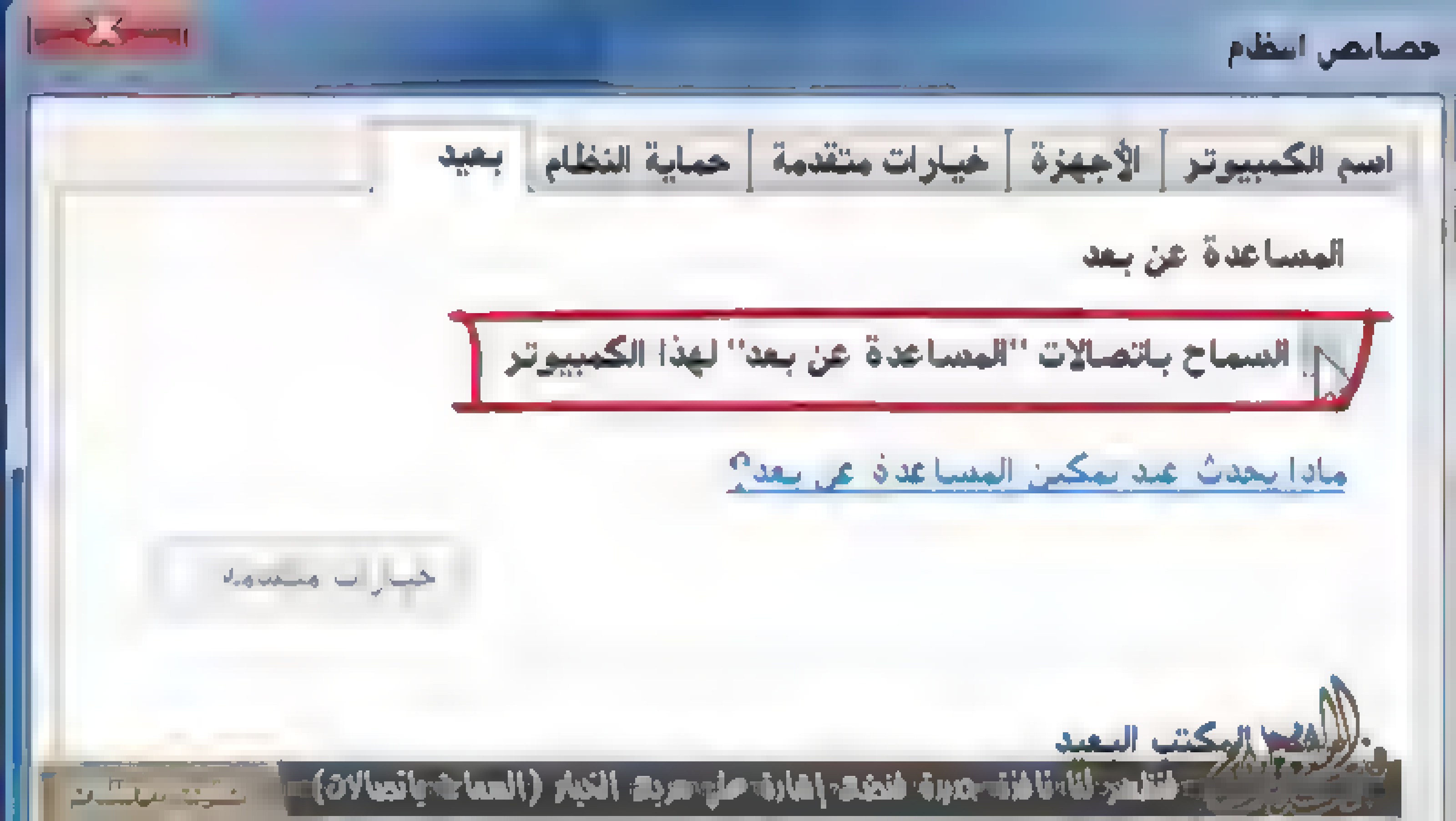
إدارة الأجهزة

إعدادات عن بعد

حماية النظام

إعدادات النظام المتقدمة

ثم تظهر لنا نافذة جديدة نضغط على (الإعدادات عن بعد)



اسم الكمبيوتر
الأجهزة
خيارات متقدمة
حماية النظام
بعيد
المساعدة عن بعد
السماح باتصالات "المساعدة عن بعد" لهذا الكمبيوتر
المكتب البعيد

انقر فوق خيار ما، ثم حدد من يمكنه الاتصال، إذا لزم الأمر.

- عدم السماح باتصالات لهذا الكمبيوتر
- السماح باتصالات من أجهزة كمبيوتر تستخدم أي إصدار من "سطح المكتب البعيد" (أقل أمانًا)
- السماح فقط باتصالات من أجهزة كمبيوتر تُشغل "سطح المكتب البعيد" باستخدام "مصادقة مستوى الشبكة" (أكثر أمانًا)

المساعدة في الاختيار

تحديد المستخدمين

ثم نضغط موافق

ما هو RDP وكيف أحصل عليه:

وهذه الشركات التي تقدم الخدمة بشكل مجاني لكن لفترة تجريبية أقصاها 7 أيام وبعد انتهاء المدة يمكنك عمل حساب جديد

ما هو RDP وكيف أحصل عليه:



وهذه الشركات التي تقدم الخدمة بشكل مجاني لكن لفترة تجريبية أقصاها 7 أيام وبعد انتهاء المدة يمكنك عمل حساب جديد

alwaysonpc.com أو Desktone.com وهناك الكثير من المواقع يمكنك البحث عنها بمحركات البحث

وسنشرح طريقة التعامل مع المواقع التي ذكرناها ونفس المبدأ مع كل المواقع ولكن يجب عليك تنصيب الجافا قبل البدء

وطبعا هناك بعض المساوئ للشركات المجانية منها البطء أو حظر بعض المواقع والخ

وطبعا لاستخدام هذه الخدمة سواء كانت مجانية أو مدفوعة يجب أن يكون لديك اتصال انترنت جيد السرعة

ما هو RDP وكيف أحصل عليه:

دعونا نشاهد هذا الشرح البسيط لطريقة الحصول على الخدمة من موقع Desktone.

New Tab

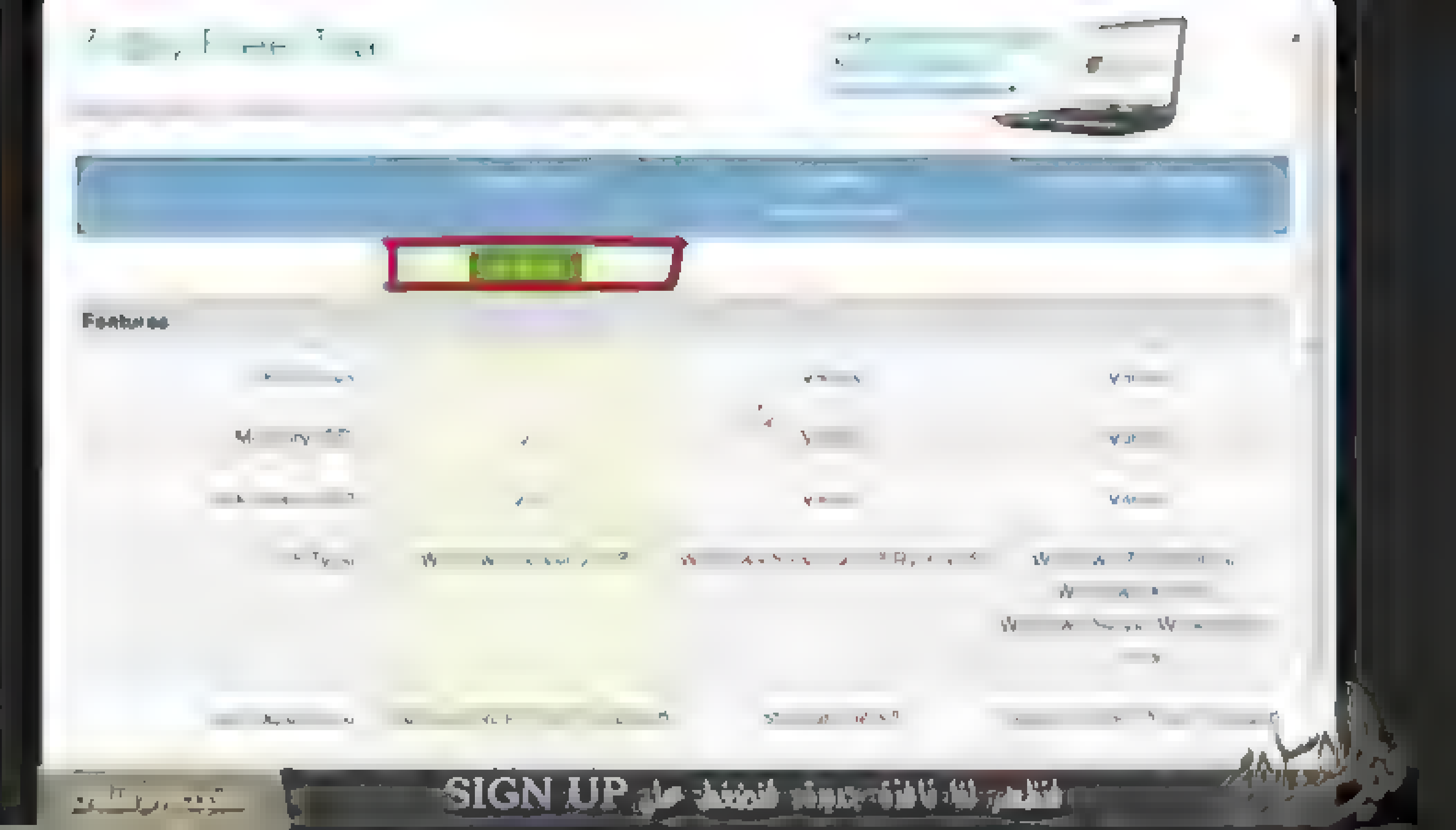
New Tab

.desktone.com



Features

SIGN UP


Features
SIGN UP

First Name

Last Name

Company Size — Select a Company Size

State — Select a State

Country — Select a Country

Are you interested in ...

Select One

Please create a username and password for your account

جولتنا لصفحة التسجيل بالموقع

First Name

Last Name

Company

Company Size — Select Company Size

Email

Phone

State — Select a State

Country — Select a Country

VMware Horizon DaaS

Please create a username and password for your account

Username

Password

سنقوم بملء الحقول ببيانات عشوائية عدا الإيميل ويمكن استخدام إيميل مؤقت

First Name

Last Name

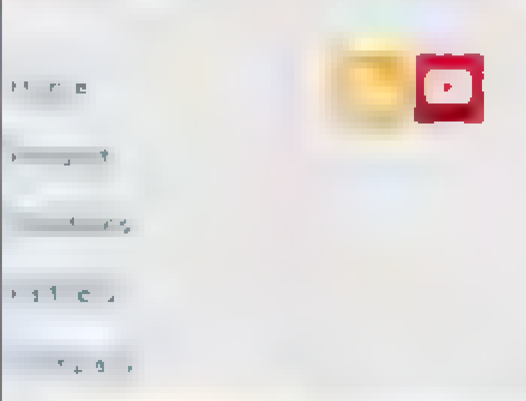
VMware Horizon DaaS
Now Supported on

Please create a username and password for your account.

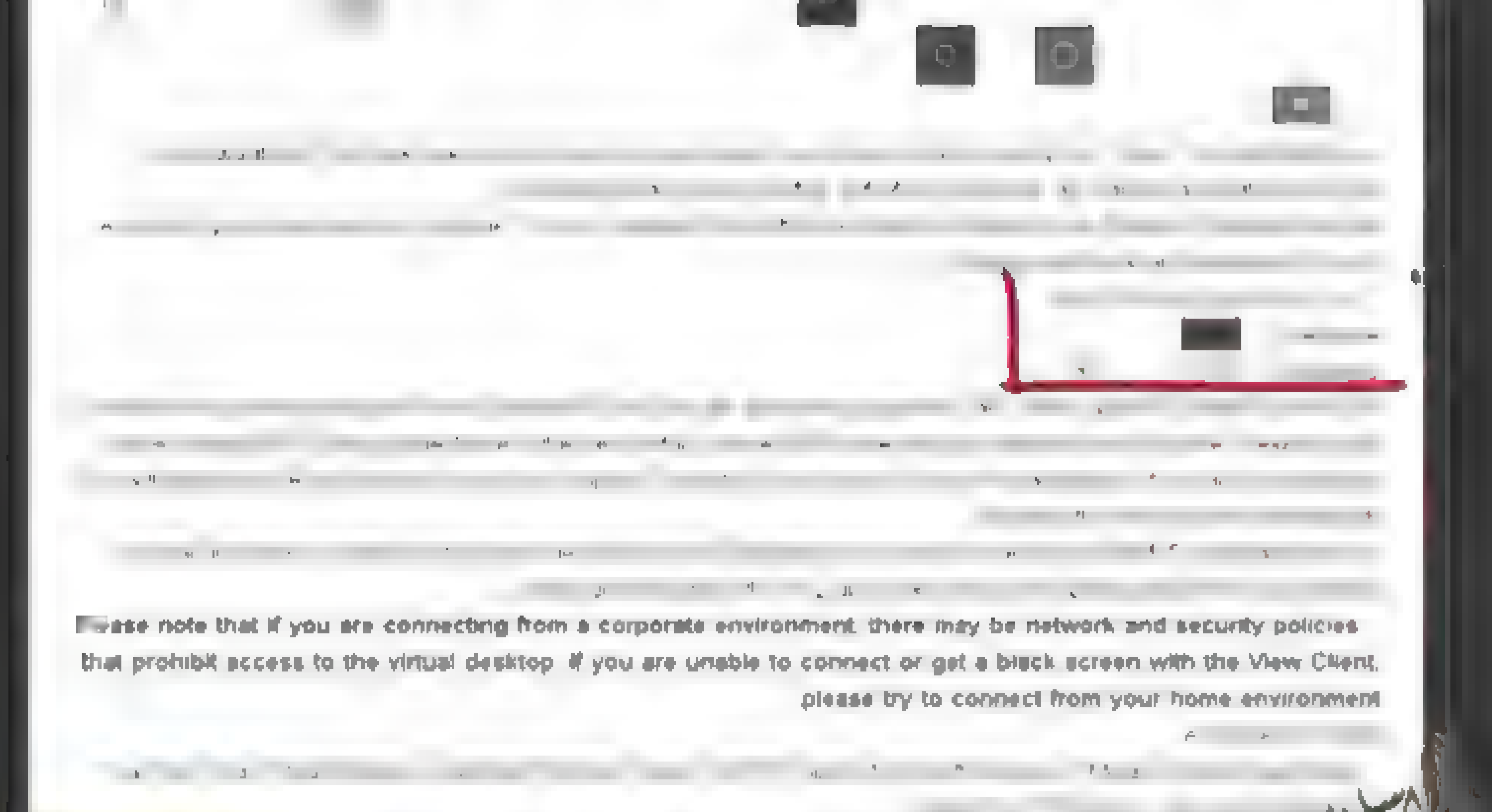
ستقوم بملء الحقول بيانات عشوائية عدا الايميل ويمكنك استخدام ايميل مؤقت

Thank You

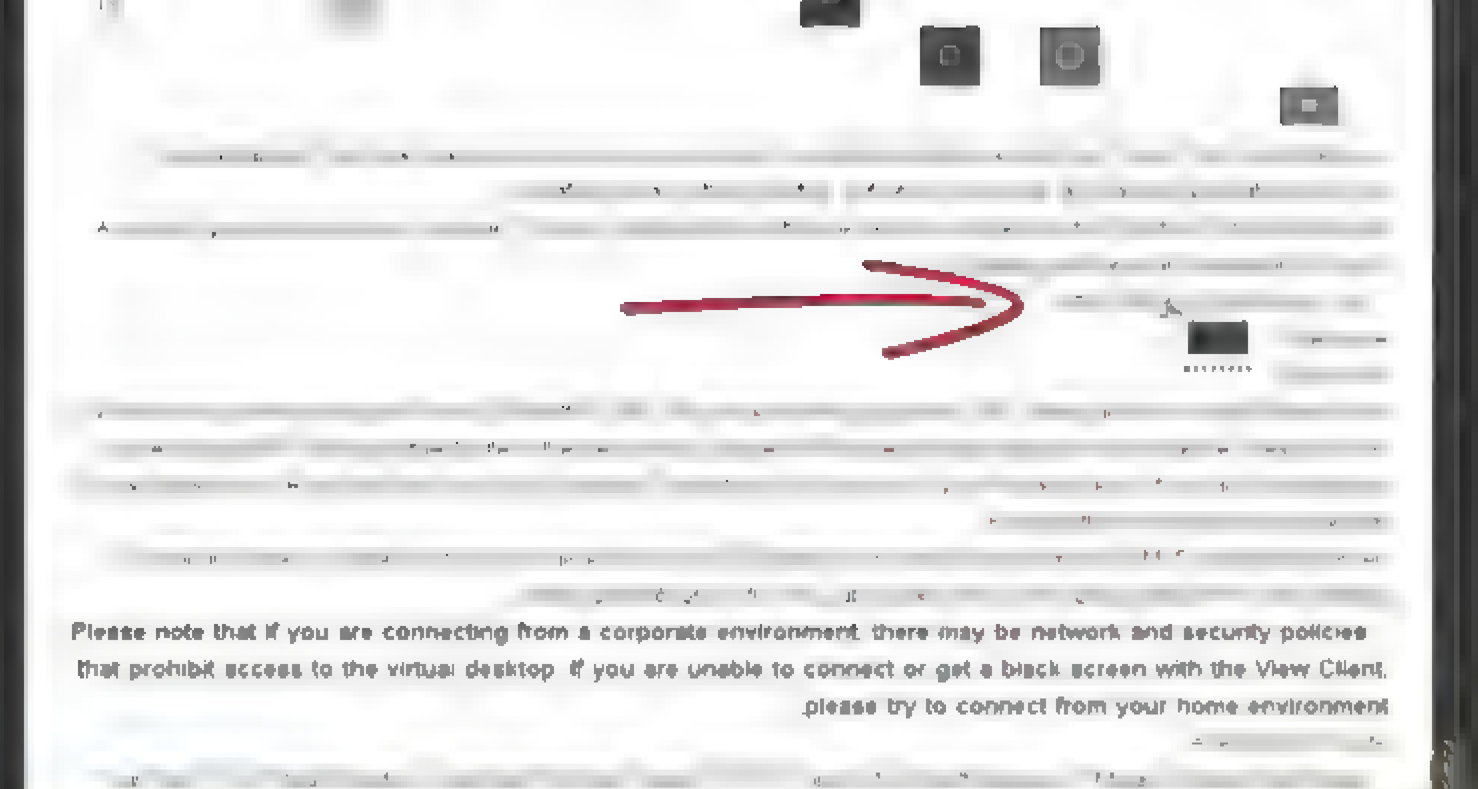
Thanks for registering for a virtual desktop. You will receive an email shortly with instructions for connection

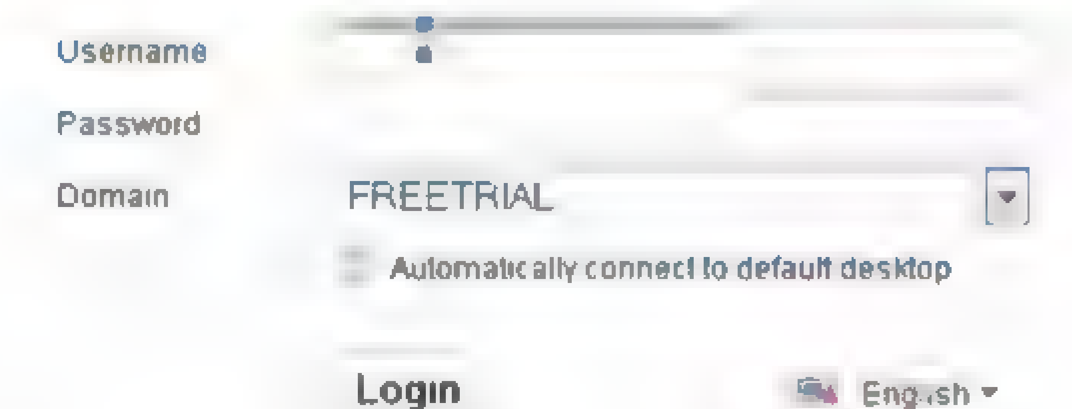






ease note that if you are connecting from a corporate environment, there may be network and security policies that prohibit access to the virtual desktop. If you are unable to connect or get a black screen with the View Client, please try to connect from your home environment


Please note that if you are connecting from a corporate environment, there may be network and security policies
that prohibit access to the virtual desktop. If you are unable to connect or get a black screen with the View Client,
please try to connect from your home environment.


Username
Password
Domain
FREETRIAL
Automatically connect to default desktop
Login
English


لا نحفظ البيانات التي سجلنا بها وحصلنا عليها الأسبق

Username

Password ●●●●●●●●●

Domain FREETRIAL

Automatically connect to default desktop

Login

English



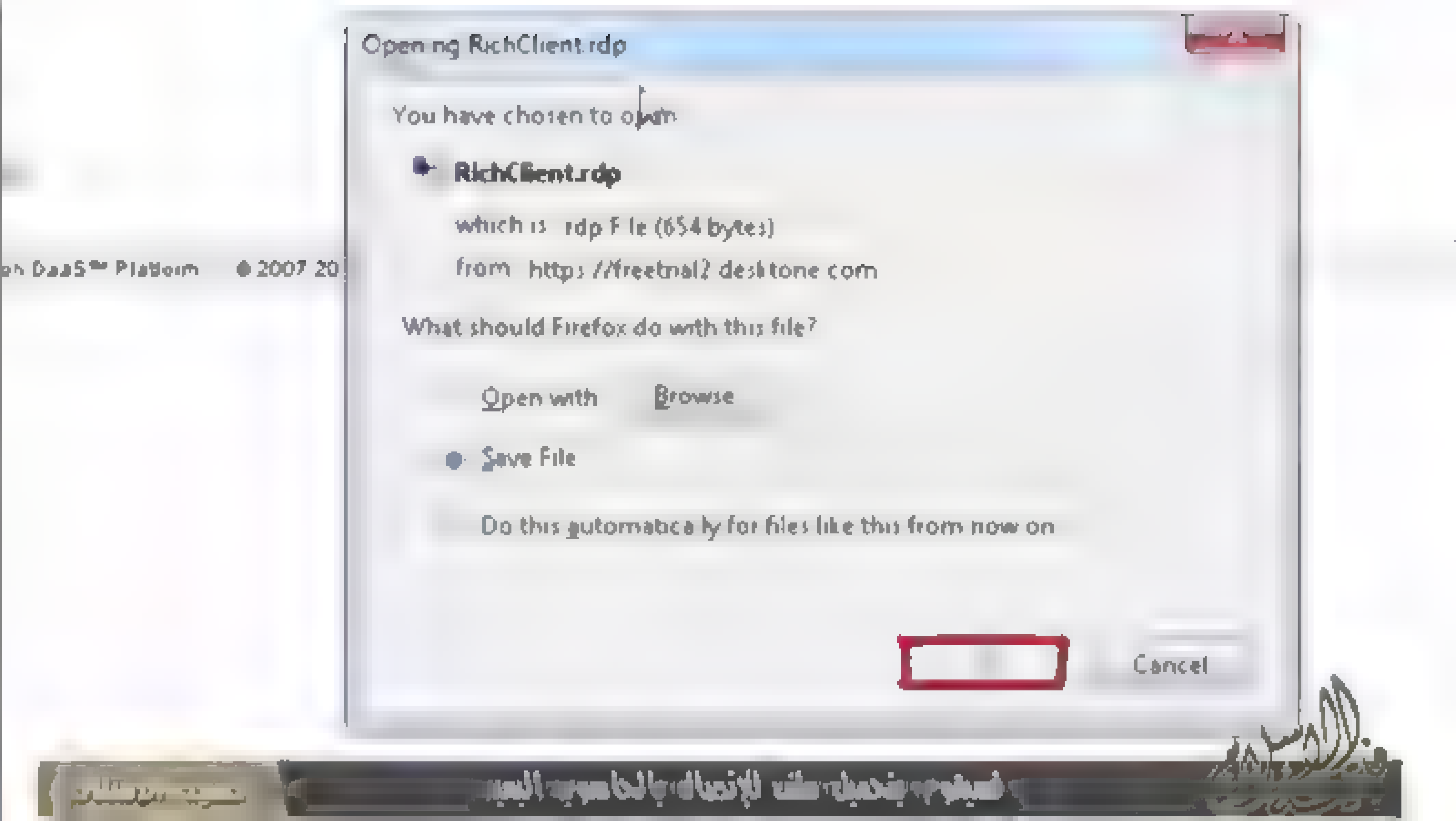


Desktops (1)

Desktop or pool name	Connect	Protocol
Freetrial		RDP



Desktop

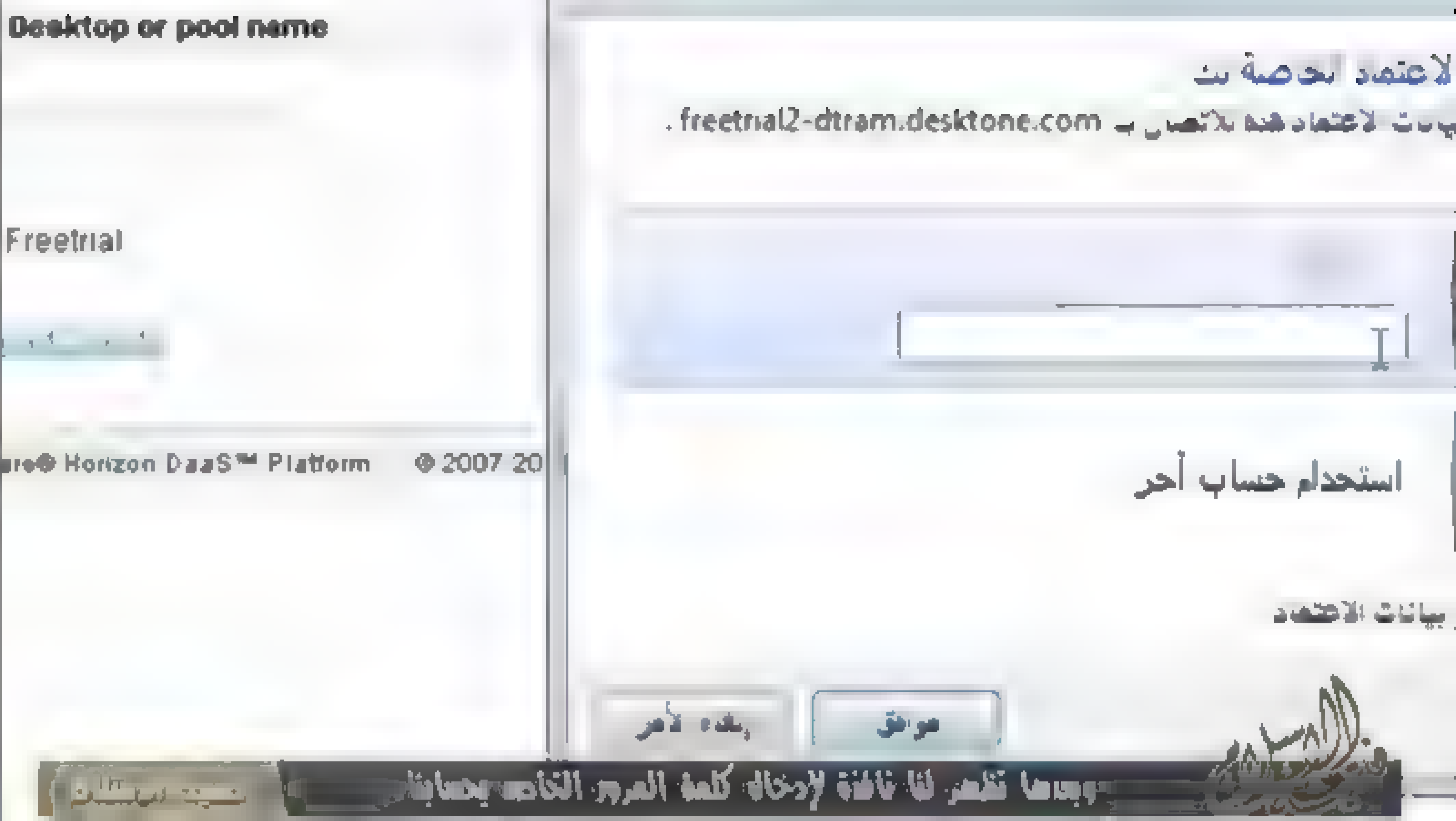


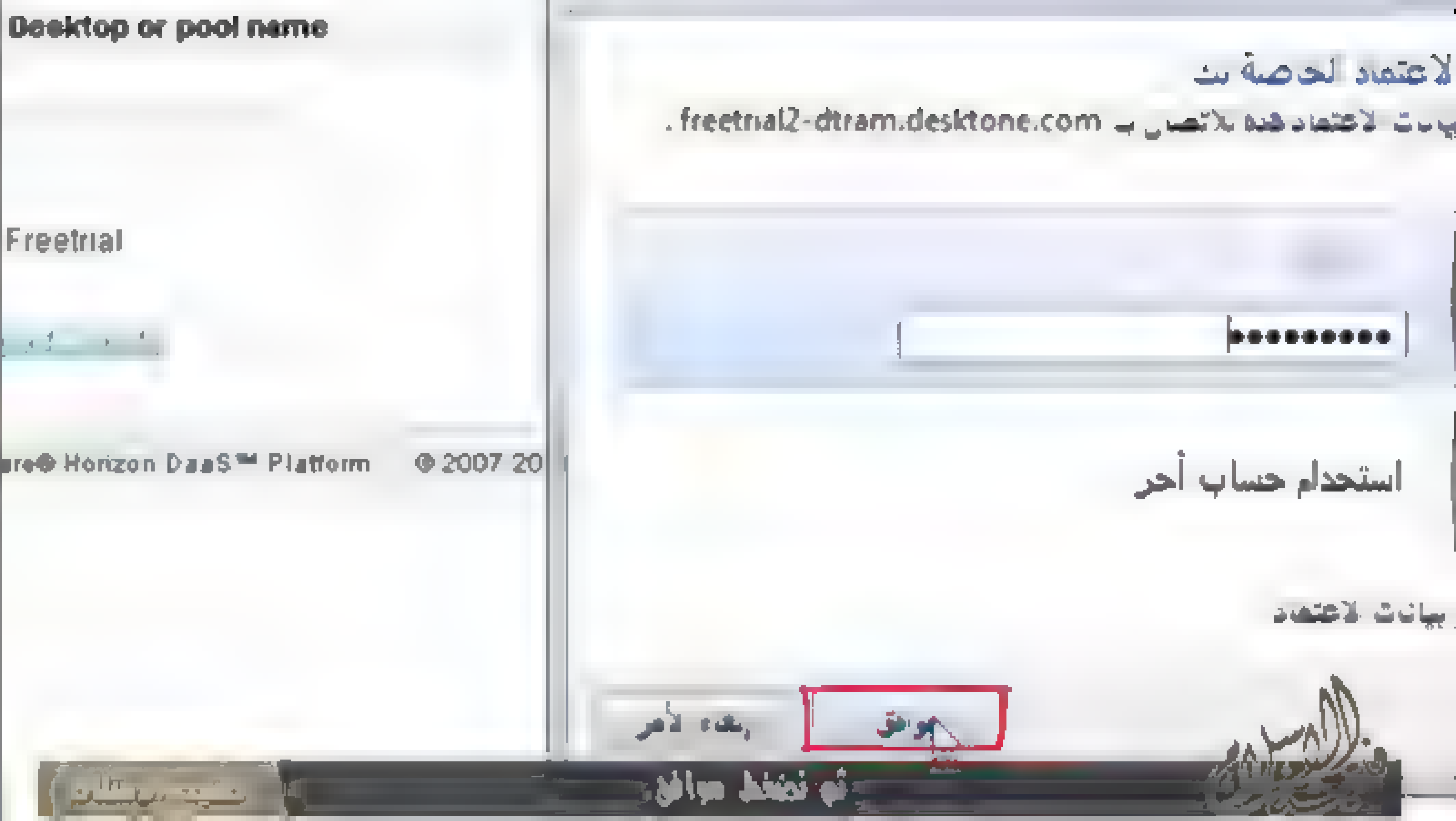
Opening RichClient.rdp
You have chosen to open
RichClient.rdp
which is rdp File (654 bytes)
from https://freetrial2.desktone.com
What should Firefox do with this file?
Open with
Browse
Save File
Do this automatically for files like this from now on
Cancel


nnect
Protocol
Power state
RDP
ware, Inc. All rights reserved


Connect
Protocol
الاتصال بسطح المكتب البعيد
يتعذر التعرف على ناشر هذا الاتصال البعيد. هل تريد الاتصال على أية حال؟
قد يؤدي هذا الاتصال البعيد إلى إلحاق ضرر بالكمبيوتر المحلي أو الكمبيوتر البعيد الخاص بك. الرجاء عدم الاتصال ما لم تكن قد أعطت علما بمصدر هذا الاتصال أو قمت باستخدامه مسبقًا
الناشر
ناشر غير معروف
النوع
الاتصال بسطح المكتب البعيد
الكمبيوتر البعيد
freetrial2-dtram.desktone.com
عدم المطالبة مرة أخرى بإجراء اتصالات بهذا الكمبيوتر
اتصال
إلغاء الأمر
فتظهر لنا رسالة تحذيرية نضغط على اتصال


Connect
Protocol
RDP
الاتصال بسطح المكتب البعيد
الاتصال بـ
freetrial2-dram.desktone.com:8037
إلغاء الأمر
يتم الآن بدء الاتصال عن بعد
© 2007 201
ثم ننتظر حتى يتم الاتصال


Desktop or pool name
freetrial2-dtram.desktone.com
Freetrial
Horizon DaaS™ Platform
© 2007 20
استخدم حساب آخر
موافق
إلغاء الأمر
وبعدها تظهر لنا نافذة لإدخال كلمة المرور الخاصة بحسابنا



Desktop or pool name
Freetrial
Horizon DaaS™ Platform
© 2007 20
freetrial2-dtram.desktone.com .
استخدام حساب أخر

RDP ▾

الاتصال بسطح المكتب البعيد

الاتصال بـ

freetrial2 diram desktone com 8037

إلغاء الأمر

يتم الآن تأمين الاتصال عن بعد

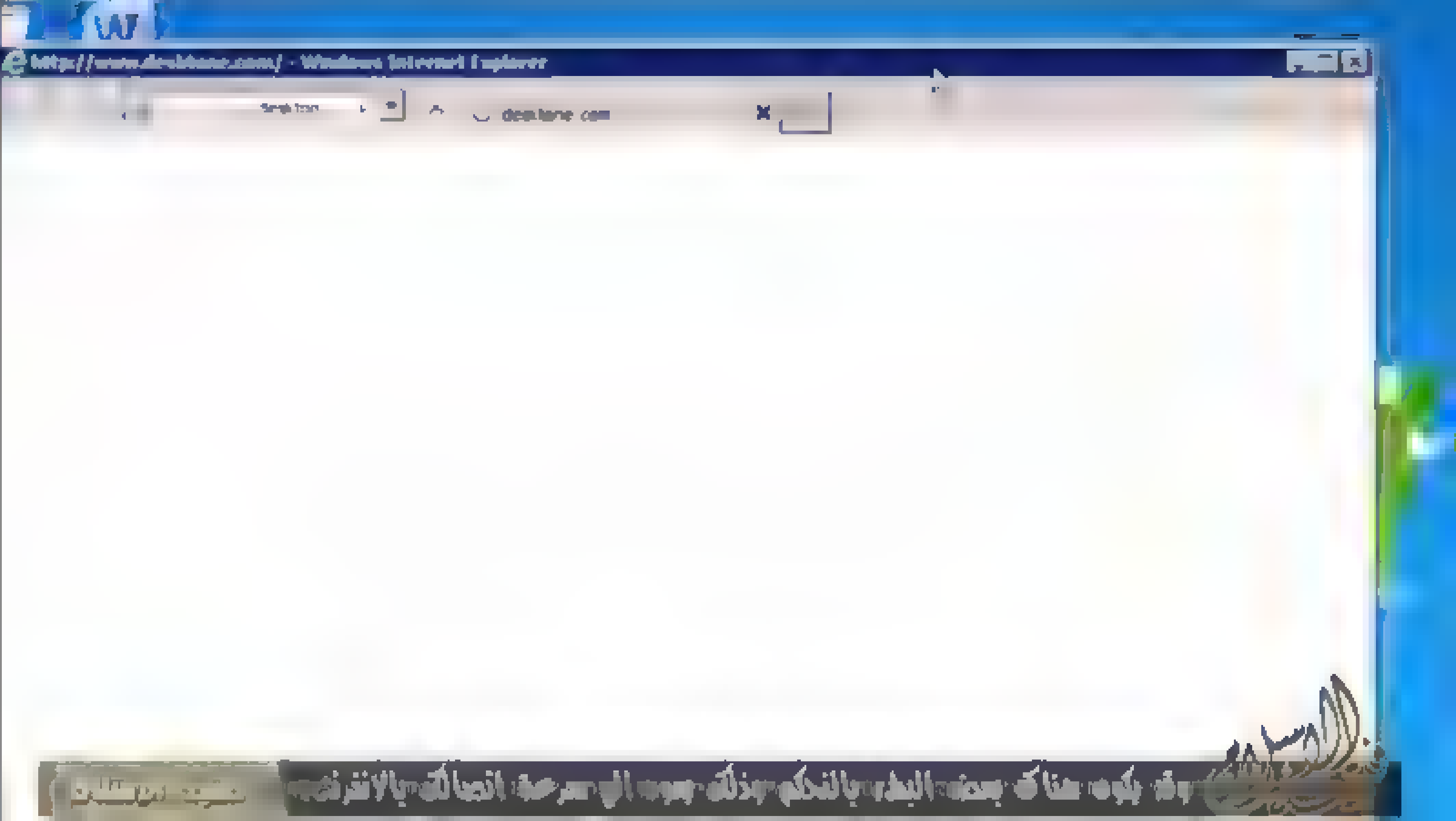
© 2007 201

ننتظر إتمام الاتصال



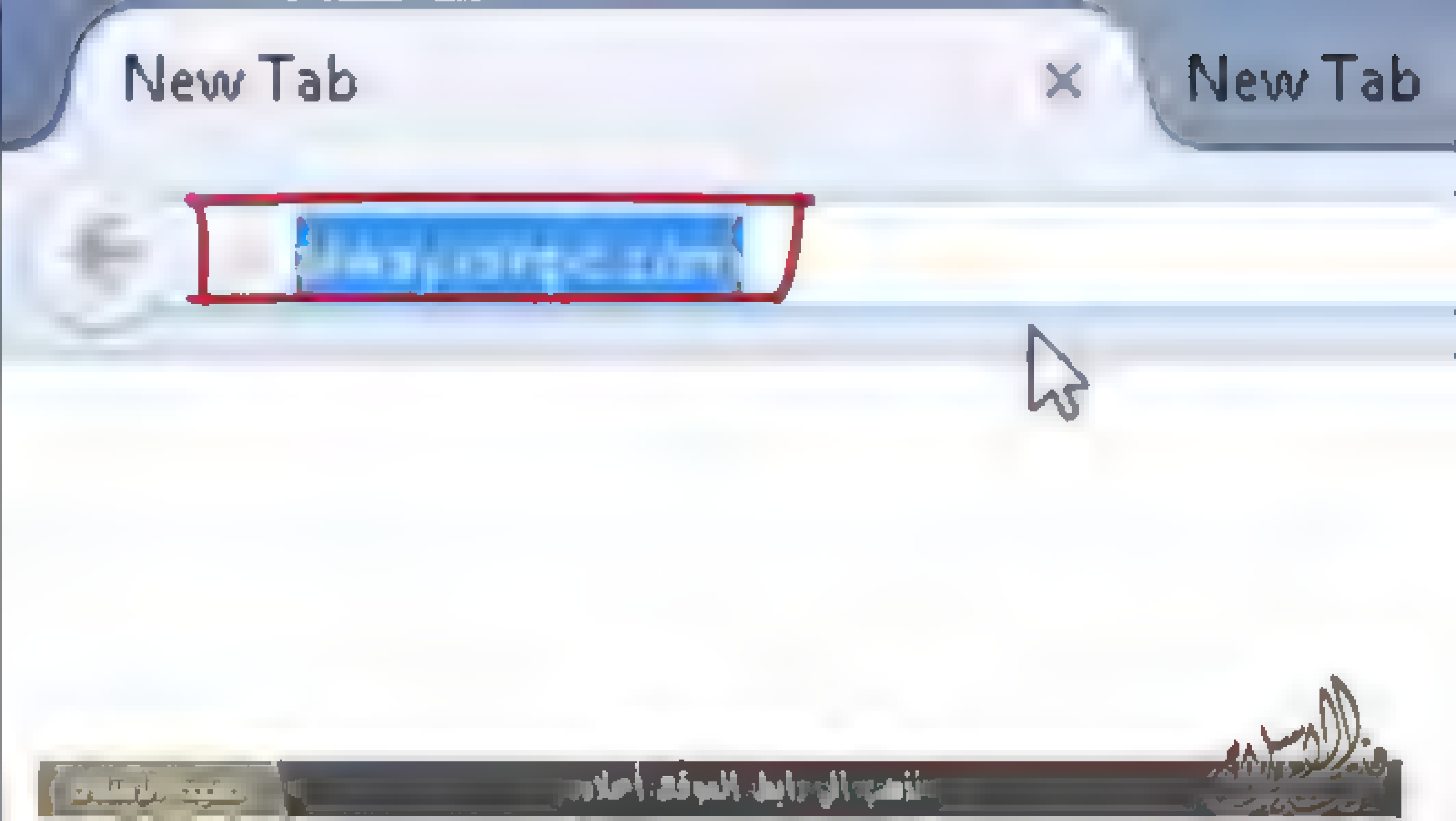

بعد إتمام الإتصال ستفتح لنا نافذة للتحكم بالحاسوب البعيد بالكامل


بعد إتمام الإتصال ستفتح لنا نافذة للتحكم بالحاسوب البعيد بالكامل


desktone.com

ما هو RDP وكيف أحصل عليه:



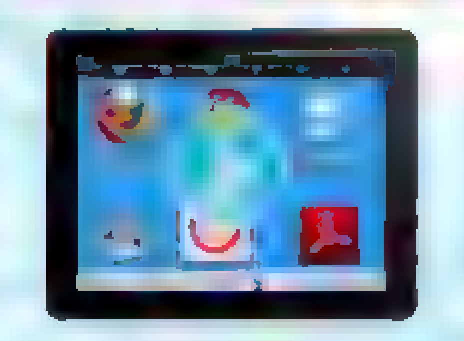

New Tab
New Tab

Language: English

AlwaysOnPC



Run Chrome, Firefox, Flash, Java, Open Office Suite & More on iPad, iPhone and Android

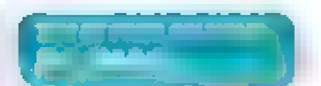




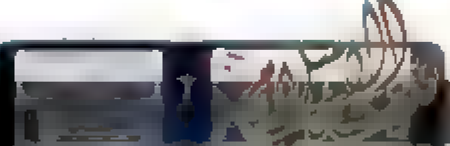












First name

Last name

Email

Retype email

Password

Retype password

Please select the location closest to you:

- US
- Europe/UK

Type the character string

I agree to the Always

فنملئ النموذج ببيانات عشوائية عدا الايميل ويمكن استخدام ايميل مؤقت

First name

Last name

Email

Retype email

Password ●●●●●●●●●●●

Retype password ●●●●●●●●●●●

Please select the location nearest to you ● Europe/Asia

Type the character string mnc3a

mc3a

✓ I agree to the Awaysoft...

Go

وبعد الإنتهاء نضع اشارة على مربع القبول ثم نضغط زر Go

AlwaysOnPC



Buy our mobile apps here



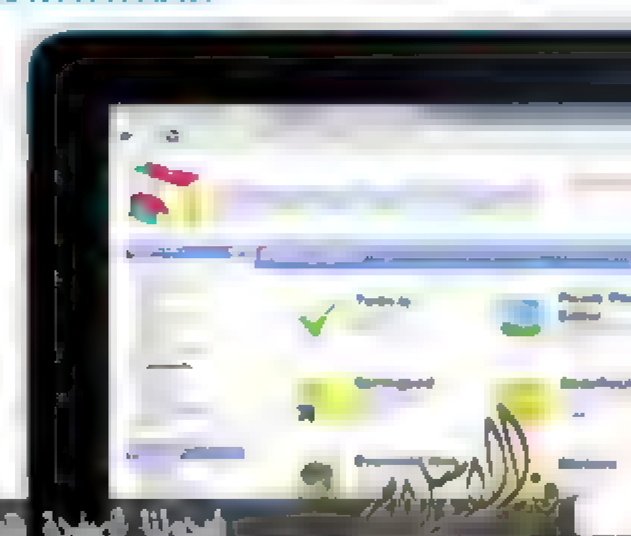
AlwaysOnPC

Congratulations: your account is now confirmed.

Facebook

Twitter

 Email



ليحولنا لصفحة يقول فيها انه تم تفعيل الحساب الخاص بنا

AlwaysOnPC



Welcome to AlwaysOnPC!

Click the [illegible] button below to launch the free Always[illegible] viewer for your [illegible]mputer

Free trial: you can try all our features for up to [illegible] minutes per session for up to five days

Already have one of our mobile Apps [illegible] the PC [illegible] Always[illegible]

PC [illegible] If you have purchased and activated [illegible] logged in at least once [illegible] mobile App, you can use the [illegible] session

Connect to my AlwaysOnPC

Have questions? [illegible] the Help button at the top of the page [illegible] contact us at [illegible]



Opening startAlwaysOnPC.jnlp

You have chosen to open:

startAlwaysOnPC.jnlp

which is: JNLP File (962 bytes)

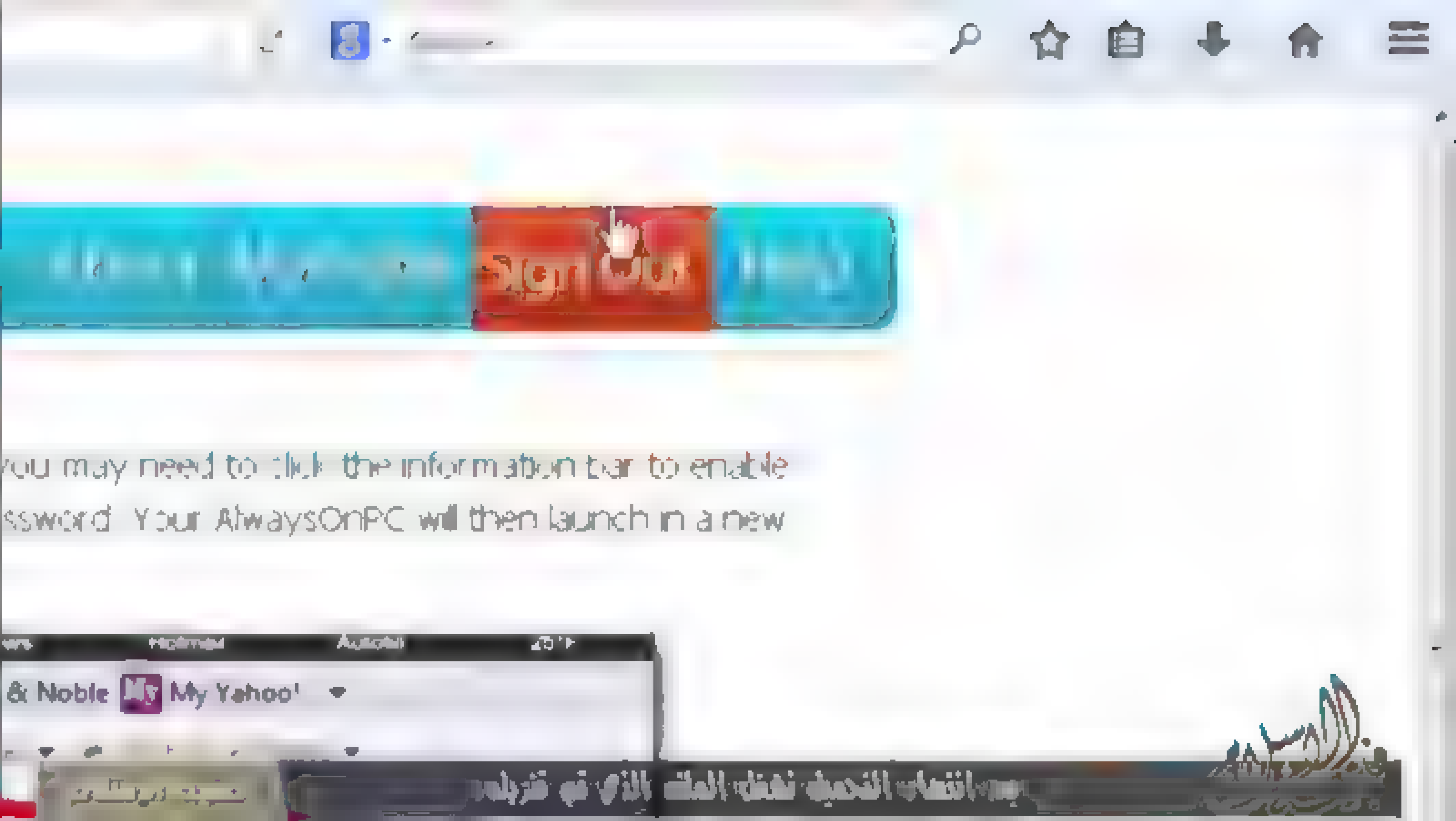
from: http://www.alwaysonpc.com

What should Firefox do with this file?

Open with Java(TM) Web Start Launcher (default)

Save File

Do this automatically for files like this from now on.


ou may need to click the information bar to enable
ssword. Your AlwaysOnPC will then launch in a new
& Noble
My Yahoo!
وبعد انتهاء التحميل نفتح الملف الذي تم تنزيله

AlwaysOnPC

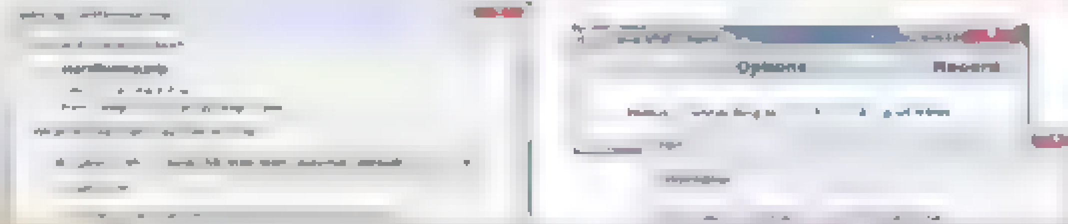



AlwaysOnPC
Options
Record
يظهر لنا مربع لإدخال البيانات التي سجلنا بها وأكملنا ثم نضغط Ok

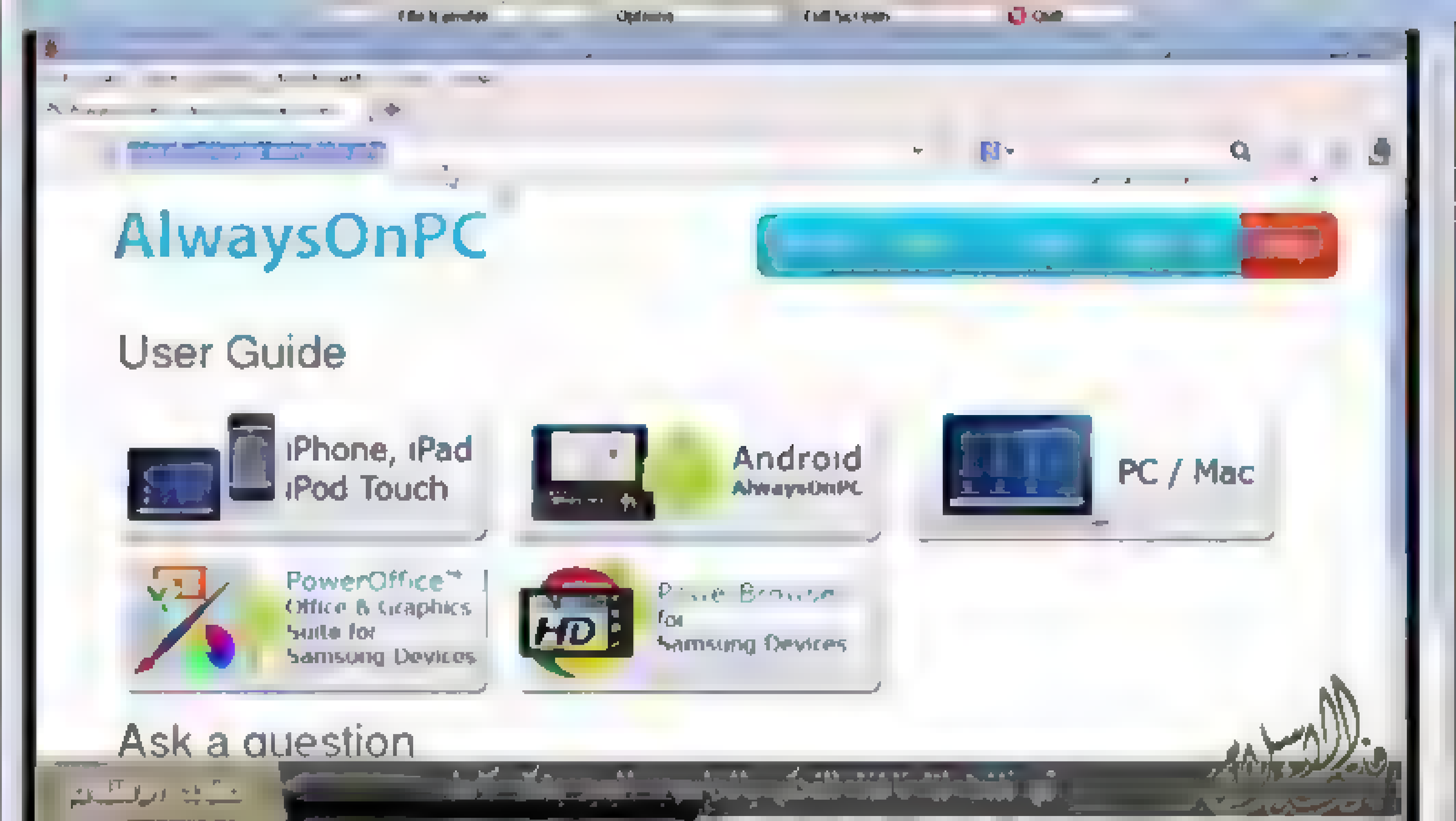
AlwaysOnPC










AlwaysOnPC
User Guide
iPhone, iPad
iPod Touch
Android
AlwaysOnPC
PC / Mac
PowerOffice
Office & Graphics
Suite for
Samsung Devices
for
Samsung Devices
Ask a question

تشفير الرسائل والملفات بشكل يدوي:

تشفير الرسائل والملفات باستخدام أنظمة التشفير المختلفة هو أمر يزيد من حماية الخصوصية والسرية في تناقل الرسائل والملفات

وتختلف أنظمة التشفير من هذه الطرق، لكن سنشرح أهم أبرزها وأفضلها، وسنستخدم برنامج أمن المجاهد لهذه الخطوات

وهو برنامج من برمجة الأخوة في اللجنة التقنية لمركز الفجر، وهذا رابط صفحة البرنامج من الموقع الرسمي:

https://alfajrtaqni.net/amn.html

وهو برنامج بسيط الاستخدام، ويعتمد بالتشفير على مفتاحين: مفتاح خاص ومفتاح عام، فأغلب أنظمة التشفير تعمل بهذا الأسلوب

المفتاح الخاص: هو مفتاح خاص بك ولا يجب أن تشاركه مع أحد ويجب أن تحتفظ به وتقوم بعمل نسخة منه في مكان مخفي

المفتاح العام: هو مفتاح تشاركه مع من تراسله، ولكن هذا المفتاح لن يستطيع فك التشفير ويستخدم في التشفير ويجب الاحتفاظ به

تشفير الرسائل والملفات بشكل يدوي:

أول ما عليك هو توليد مفتاح خاص بك ووضع كلمة سر له بالعربية أو الإنجليزية وتخزينه لديك

ومشاركة المفتاح العام للتشفير مع الشخص الذي تريد مراسلته، فكل شخص تريد مراسلته عليك أن تملك مفتاحه العام وهو كذلك

ويمكنك امتلاك أكثر من مفتاح على حسب حاجتك

بعد تحميل البرنامج افتحه بمجلد خاص به واشغله، وعند تشغيله سيتولد ملف بجانبه اسمه «مفاتيح»

بعد فتح البرنامج أول مرة اذهب إلى «إدارة المفاتيح» ثم اضغط على «إنتاج مفتاح»

ثم قم بوضع حجم المفتاح كما تريد واسم له وكل ما تريد مع الانتباه لنوع اللغة، ثم اضغط على زر «إنشاء المفتاح»

لمعرفة المزيد عن البرنامج وبتفصيل أكثر منه، يمكنكم الاطلاع على الكتيب المصور المرفق مع البرنامج

تشفير الرسائل والملفات بشكل يدوي:





دورة التخفي والتصفح الآمن للإنترنت.

خاتمة الدورة.



ختامية الدورة :

بعد أن قدمنا ما يسر الله لنا في هذه الدورة من طرق للتخفي والتصفح الآمن

نُعيد ونُذكر بأنه لا يوجد شيء اسمه حماية كاملة متكاملة وهذا ضرب من الخيال.

فكُل ما تقوم به من خطوات وطرق ما هو الا تعقيد المهمة بشكل أكبر على المُتجسسين من هاكرز أو حكومات

فعند استخدامك أساليب التشفير والتعامل بحرص كامل فأنه سيصعب التجسس عليك الى حد الشبه مستحيل

وفي النهاية كل ما ذكرناه في هذه الدورة ما هو الا طرق للحماية اثناء التصفح واستخدام الإنترنت

ولم نتطرق الى طرق وسُبل حماية الأجهزة من الاختراق والتجسس, وتعمدنا ذلك

لأننا أردنا جعل ذلك بدورة مخصصة ان يسر الله لنا, وان وجدنا تفاعل جيد مع هذه الدورة



ختامية الدورة :

وان شاء الله سننتظر لفترة حتى نلمس التفاعل مع هذه الدورة, وان وجدنا من هو مهتم بهذه الأمور ستكون دورة حماية الأجهزة وتحصينها هي الدورة القادمة بإذن الله.

وبحال وجود أي استفسارات عن هذه الدورة, يرجى مراسلتنا على حساباتنا على الشبكات الاجتماعية في تويتر أو فيس بوك وسنجيب على استفساراتكم قدر الإمكان بإذن الله .

وبعد ذلك فأن أصبنا في هذه الدورة فهو من الله وأن أخطأنا فهو من أنفسنا والشيطان.

ونسأل الله أن يكون هذا العمل خالصاً لوجهه الكريم, ونسأل الله الثبات والنصر لإخواننا المجاهدين بكل بقاع الأرض.

ونرجو كل من تابع هذه الدورة أن ينشرها على حساباته وفي كل مكان لتصل الى أكبر عدد ممكن من المسلمين.



ختامية الدورة :

فالدال على الخير له نفس أجر فاعله, فتخيل أنك بمجرد النشر ستأخذ نفس أجر مُعد هذا العمل ؟

هذه الدورة ثمرة عمل ودراسة لفترة طويلة, الله أعلم بها وأعلم بحال من أعدها, فهل ستبخل علينا بدعوة بظهر غيب ؟

ونسأل الله أن تكون أعمالنا لوجهه الكريم, ولا نريد من أحد جزاء ولا شكورَ, فقط لا تنسونا من صالح دعائكم

وانتظرونا بأعمال قادمة بإذن الله.

والسلام عليكم ورحمة الله وبركاته